Universidad Carlos III de Madrid

Máster Universitario en Derecho en las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información
2015-2016

Trabajo Final de Máster

"Informe sobre la viabilidad jurídica de un software para la gestión médica en la nube"

Laura Morillo Matilla

Tutora

María Nieves de la Serna Bilbao

Madrid, 1 de Julio de 2016

***Palabras clave*:** Cloud Computing, protección de datos de carácter personal, Historial Médico Electrónico, dato sanitario, autonomía del paciente, responsable del tratamiento, encargado del tratamiento, subencargado del tratamiento, Transferencias Internacionales de datos.

***Resumen*:** El presente trabajo pretende ser un análisis integral sobre la viabilidad jurídica de un proveedor de servicios en la nube para la gestión del Historial Médico Electrónico en Clínicas y Centro Médicos privados. Para ello, se realiza un análisis estructural de todos los elementos que integran esta prestación de servicios, empezando por la configuración del Cloud Computing y los elementos que lo componen para continuar por el Historial Médico Electrónico y todas las implicaciones en materia de protección de datos que de él se derivan, incluyendo la identificación, el acceso, tratamiento de datos, sujetos que intervienen en el mismo así como las medidas de seguridad que le son aplicables. Finalmente, el informe se concluye con un diagnóstico sobre la viabilidad del mismo en el ordenamiento jurídico español.

ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

ARCO (derechos): derechos de acceso, rectificación, cancelación y oposición

Art.: Artículo

CCT: Cláusulas Contractuales Tipo

CDFUE: Carta de Derechos Fundamentales de la Unión Europea

EEE: Espacio Económico Europeo

HME: Historial Médico Electrónico

LBAP: Ley 41/2002 de 14 de Noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

RDLOPD: Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

TI: Transferencias Internaciones de datos

TJUE: Tribunal de Justicia de la Unión Europea

ÍNDICE

ANEXOS

1. PRESENTACIÓN DEL CASO

1.2. Objeto del informe

El presente informe tiene como objeto el análisis y estudio de la viabilidad jurídica del software de gestión médica en la nube desarrollado por GESTCARE iCLOUD, S.L., (en adelante, GESTCARE iCLOUD) y sus principales implicaciones legales en materia de protección de datos.

Este software en la nube se dirige a los centros médicos, entre los que pueden incluirse desde consultas pequeñas, clínicas y centros médicos más grandes del sector privado.

En este sentido, podrán acceder al Historial Médico Electrónico (HME) en la nube tanto el los médicos y demás profesionales sanitarios como el personal administrativo y otros trabajadores que por razón de su actividad profesional estén autorizados para acceder a la parte del HME que les corresponda. Cada uno de ellos cuenta con un perfil personal delimitado y sujeto a medidas de seguridad y controles de acuerdo a la tipología y nivel de protección de los datos tratados tendientes a garantizar y proteger los datos contenidos en el mismo.

Además, los propios pacientes también cuentan con un perfil personalizado mediante el cual pueden acceder a su HME, de tal modo que es posible consultar la información en él contenida, pruebas y diagnósticos, pedir cita, o incluso ser atendidos en cualquier momento y lugar a mediante del servicio de geolocalización. Todo ello puede llevarse a cabo a través de cualquier dispositivo electrónico desde el que se acceda, ya sea teléfono móvil, pc, tableta electrónica, etc.

1.2. Ámbito de aplicación

El ámbito de aplicación de este informe son todas las clínicas y centros médicos que contraten los servicios de GESTCARE iCLOUD dentro del territorio español y las normas jurídicas que por tal condición le sean aplicables.

2. CLOUD COMPUTING

2.1. ¿Qué es el Cloud Computing?

En los últimos tiempos, y más especialmente desde los años 2010 y 2011, existe una creciente tendencia a externalizar servicios de todo tipo en la nube, pues muchas empresas, ya sean multinacionales, medianas empresas, pymes o incluso usuarios autónomos, se han apuntado a este nuevo fenómeno llamado *"Cloud Computing"*, debido al gran atractivo y grandes beneficios que presenta este nuevo modelo de gestión de los recursos a través de internet. Pero, ¿qué es el Cloud Computing?

No existe una sola definición de Cloud Computing, aunque la más acertada y comúnmente aceptada es la que proviene del Nacional Institute of Standards and Technology (NIST) de los Estados Unidos que lo define como:

"Un modelo que permite acceder de forma cómoda y ubicua, a petición del usuario, a una serie de recursos informáticos compartidos y configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden suministrar con rapidez y distribuir con un esfuerzo mínimo de gestión o interacción del proveedor de servicios."[1]

La información se almacena permanentemente en servidores de Internet del proveedor y cuando es requerida por un cliente se envía a los equipos del mismo, pudiendo contar con ella en todo momento a través de la red. Una de las principales ventajas de este modelo es que no se necesita tener los datos almacenados físicamente en los ordenadores, sino que el hardware que tradicionalmente era integrado físicamente en los mismos, ahora es proporcionado por el proveedor en la nube.

[1] NIST, Mell, P. y Grance, T.: *The NIST Definition of Cloud Computing*, 2011, p. 2 en http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Por lo tanto, las principales notas características de este modelo son las siguientes:

a) Autoservicio a demanda según las necesidades empresariales de cada momento. Es decir, el usuario puede incrementar la capacidad de almacenamiento, el tiempo de utilización de los recursos o capacidad de procesamiento de forma dinámica y según sus necesidades.

b) Modelo multiposesión. Los recursos del proveedor son dispuestos de una manera común para servir a múltiples usuarios, de modo que los recursos físicos y virtuales son agrupados conjuntamente y asignados de manera dinámica a los diferentes usuarios, de acuerdo a sus necesidades y capacidades contratadas. Además, esta asignación se hace de manera ubicua, de modo que los servicios son prestados desde diferentes lugares sin que el cliente tenga conocimiento exacto de en qué lugar físico se encuentran sus datos.

c) Acceso a través de la red a los recursos contratados con el prestador de cloud desde cualquier dispositivo que tenga acceso a internet ya que, como hemos mencionado con anterioridad, tanto el *hardware*, como en la mayoría de casos, el *software*, será proporcionado por el proveedor de los servicios cloud.

d) Flexibilidad y optimización de los recursos de manera automática. La asignación de recursos es altamente escalable ya que se lleva a cabo automáticamente, de acuerdo a las directrices establecidas entre cliente y proveedor. De esta manera, en muchas ocasiones el cliente tiene la sensación de que los recursos a su disposición son ilimitados.

Asimismo, el cliente puede seguir, controlar y acceder en todo momento a la información referente la asignación de estos recursos por parte del proveedor, dotando así de una enorme transparencia a la relación contractual de prestación de los servicios en la nube.

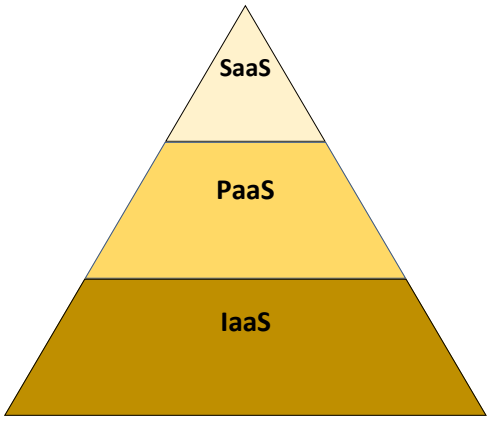
2.2. ¿Qué tipos de Cloud existen?

Una vez ha quedado bien delimitado qué es el Cloud Computing es preceptivo establecer los diferente tipos de Cloud existentes en el mercado, ya que se debe determinar cuál es el más adecuado para los servicios que se van a llevar a cabo a través del software para la gestión médica desarrollado por GESTCARE iCLOUD, tanto en lo referente al tipo de servicio como al despliegue llevado a cabo.

2.2.1. Según modelo de servicio

Los servicios de Cloud Computing se estructuran de manera piramidal, de acuerdo al desarrollo del servicio que van a prestar. Existen tres tipos de servicios:

a) Software como servicio (SaaS). El cliente utiliza las aplicaciones completas y diseñadas por el proveedor de servicios en la nube. Se pone a disposición de los clientes el software final que va a ser utilizado por los mismos de modo que el software que reside en una sola infraestructura puede ser utilizado por múltiples clientes.



"*Estructura de los servicios en Cloud según modelo de servicio".* Fuente: elaboración propia**.**

b) Plataforma como Servicio (PaaS). El cliente utiliza el servicio Cloud como una plataforma de desarrollo del software que cuenta con herramientas de programación que el proveedor pone a su disposición. Así, el cliente puede desarrollar sus propias aplicaciones o

aplicaciones de terceros sin tener que instalar estas herramientas en sus propios equipos, accesibles a través de internet y muchas veces, sin necesidad de conocimientos especializados.

c) Infraestructura como Servicio (IaaS). En la base de la pirámide se encuentra esta modalidad de Cloud, en la cual el cliente solo cuenta con la infraestructura básica - capacidad de almacenamiento, procesamiento y redes - sobre la cual podrá desplegar tanto sistemas operativos (plataformas) como software específico (aplicaciones).

2.2.2. Según modelo de despliegue

El despliegue de los servicios se refiere al grado de gestión y control de los entornos tanto por el proveedor como por los clientes. Podemos distinguir principalmente entre los siguientes modelos:

a) Nube privada. Es aquella de uso exclusivo por un solo cliente, el cual normalmente decide cuántos usuarios quedan autorizados para utilizarla. Puede ser gestionada por el mismo titular o por un tercero, pudiendo estar físicamente tanto sus instalaciones como fuera de ellas. Este tipo de nube dota a los sus clientes de un alto grado de seguridad y menor dependencia con el exterior pero cuenta con unos costes más elevados.

Dentro de la misma, existen tres subtipos de nube privada. La primera de ellas es la denominada **nube dedicada**, en la cual la infraestructura está gestionada por la propia organización tanto en lo referente al centro de datos como al personal; **nube mancomunada**, la cual está gestionada en el establecimiento del proveedor siguiendo los términos contractualmente establecidos; y la denominada **nube gestionada**, en la que la infraestructura es propiedad del cliente pero es gestionada por una tercera parte.

b) Nube pública. Es aquella que atiende a una pluralidad de clientes y que es gestionada por un mismo prestador de servicios desde una infraestructura común

para todos los usuarios. Este tipo de nube cuenta con una alta dependencia del exterior, así como un grado muy limitado de control y supervisión de la actuación del proveedor por parte del cliente, que suele estar basada en contratos de adhesión de este último a los servicios del primero; motivos que explican por qué los costes suelen ser son muy reducidos.

c) Nube comunitaria. El uso se realiza exclusivamente por aquellos clientes que conforman una comunidad de organizaciones que mantienen objetivos similares. Pueden ser gestionadas por una de esas organizaciones o por terceros, independientemente de dónde se encuentre establecida físicamente la estructura.

d) **Nube híbrida.** Es aquella que comparte elementos de los tres modelos anteriormente explicados. Por ello, los clientes pueden ser propietarios de unas partes de la nube y compartir otras de manera flexible y de acuerdo a sus necesidades.

2.2.3. Propuesta de modelo para GESTCARE iCLOUD

De acuerdo a la descripción del caso y sin perjuicio del posterior desarrollo de sus otros componentes, nuestra propuesta para GESTCARE iCLOUD es la siguiente:

En cuanto al modelo de servicio, no cabe duda de que el caso que nos ocupa se trata de un **Software Como Servicio (SaaS)** desde su diseño, pues este proveedor de servicios en la nube dota a sus clientes tanto de la infraestructura como de las aplicaciones concretas a través de las cuales se lleva a cabo el programa de gestión. Es decir, en este caso, el proveedor cuenta con el producto final que va a poner a disposición de sus clientes sin que sea necesario desarrollo posterior por los mismos.

En cuanto al modelo de despliegue, tenemos una doble propuesta:

- Primeramente, aconsejamos que para garantizar la seguridad de los servicios que contrata con sus clientes, GESTCARE iCLOUD utilice la modalidad de **nube**

privada, ya que los datos que se van a tratar a través del software del que provee a sus clientes deben protegerse con mucha cautela, siendo altamente sensibles aquellos datos que contienen información sanitaria. Este modelo proporcionará a los mismos las garantías de seguridad y disponibilidad necesarias para el desarrollo de su actividad. Sin embargo, estas garantías llevan aparejado un coste económico alto, así como una posible dificultad técnica y de recursos para su organización, cuestiones que el proveedor debe tener en cuenta antes de comercializar su producto.

- Una segunda propuesta más acorde a la calidad/precio de los servicios, pero al mismo tiempo protegiendo cautelosamente la seguridad de los datos - especialmente de aquellos más sensibles - es ofrecer un modelo de **nube híbrida**, el cual permita la combinación de elementos tanto de nube pública como privada. De este modo, podrá ofrecer un servicio a través del cual se compartan a través de nube pública aquellos datos relativos a la gestión administrativa que contengan datos de nivel básico (datos de contacto del paciente, citas, pagos) contenidos en el Historial Médico Electrónico (HME) y ofrecer a través de la nube privada los servicios que traten datos especialmente protegibles y de carácter sanitario. De este modo, se reducirán los costes económicos y en general, la destinación de recursos respecto a la nube privada, pero se seguirán manteniendo altas garantías de protección para los datos más sensibles.

- **No es aconsejable que se utilice un modelo de nube pública** para la gestión del HME, ya que los datos contenidos en estos ficheros necesitan grandes medidas de control y protección. Así, aunque la nube pública represente un coste económico mucho más bajo para los clientes, éstos también tendrán en cuenta la calidad, transparencia y seguridad de los datos, factores clave a la hora de que los mismos se decidan a adquirir los servicios de un proveedor específico en Cloud.

2.3. Software en la nube para la gestión médica.

En las últimas décadas hemos visto como paulatinamente, las clínicas y centros médicos han pasado de gestionar sus archivos en soporte papel para pasarlos a soporte electrónico, utilizando aplicaciones instaladas en sus ordenadores locales. Pues bien, de acuerdo al estado de la tecnología y su constante evolución, la utilización del Cloud Computing para prestar este tipo de servicios ha constituido una verdadera y valorable opción, permitiendo hacer la gestión médica mucho más fácil, accesible y a un menor coste tanto económico como técnico, pues, como acabamos de ver, con una simple conexión a internet se podrá acceder al servicio de gestión médica en la nube sin necesidad de la instalación técnica de los programas por parte de un profesional, tal y como venía haciéndose hasta ahora.

Los principales beneficios del Cloud Computing para la gestión médica son los siguientes:

- **Costes de entrada reducidos.** No es necesaria la instalación de un hardware que sirva de infraestructura a este software en la nube, ni de almacenaje ni de ningún otro componente adicional. Esto significa, en primer lugar, la reducción de barreras de entrada a nuevos actores que hasta ahora no podían permitirse el acceso al mercado debido a los costes que implicaba la informatización de los sistemas. Pero además, también supone una puerta abierta a la modernización más rápida, integradora y económica para aquellos centros que ya disponían de gestión médica en los ordenadores locales, y que llevarán como consecuencia la reducción de los gastos en la empresa.
- **Coordinación de la gestión sanitaria entre diferentes centros.** El hecho de disponer del HME en la nube también supone la posibilidad de que los datos contenidos en el mismo puedan ser compartidos, con el consentimiento del paciente, por todos aquellos profesionales sanitarios que se requieran para una correcta y más eficiente asistencia médica a los pacientes. Este podría ser el caso de un paciente que en el mismo centro o en centros adscritos a la misma red sanitaria, cuente con asistencia sanitaria de diferentes especialidades médicas en las que sea tratado, de

tal modo que éste pueda coordinar en un mismo HME todos los datos de salud que conformen su Historia Clínica.

- **Interoperabilidad.** En consonancia con el punto anterior, es importante garantizar que el software que ofrece GESTCARE iCLOUD sea interoperable, en la medida de lo posible, con otros proveedores que realicen idénticos servicios. Éste hecho será especialmente relevante cuando los clientes decidan finalizar la prestación de los servicios con un proveedor de gestión médica en la nube y migrar los datos a GESTCARE iCLOUD (y viceversa). Asimismo, para facilitar a sus clientes la gestión de los recursos, este proveedor de servicios deberá, ya desde el diseño, ser compatible con todo tipo de sistemas operativos (Android, Windows, IOS, Linux…), con el fin de hacer posible el acceso al HME desde cualquier dispositivo, tanto por parte de los profesionales del centro médico como por parte de los pacientes.

  Es por ello que aconsejamos a GESTCARE iCLOUD que haga posible el acceso a sus servicios a través de un navegador web (sin perjuicio de las aplicaciones que puedan utilizarse.

- **Modularidad.** El Cloud Computing constituye un servicio "a la carta" a través del cual cada centro podrá adaptarlo de acuerdo a sus necesidades. Debido a que este software está especialmente diseñado para el ámbito médico, cuenta con herramientas moldeables y diseñadas para tal fin. De este modo, se supera la barrera estática de los softwares diseñados para ser contenidos en una estructura de hardware local.

- **Actualizaciones y copias de seguridad diarias y automatizadas.** Una de las ventajas de este software en la nube es que las actualizaciones se hacen de manera automática, sin necesidad de la intervención humana, para que pueda estar a punto en cualquier momento. Lo mismo ocurre con las copias de seguridad. Es por ello que los datos estarán guardados y pueden ser recuperados en todo momento y ante cualquier incidencia.

El art.94 RDLOPD establece que en los archivos que contienen datos de nivel alto, como es el caso de los datos de salud, deben hacerse copias de seguridad, como mínimo, semanalmente, aunque lo ideal es que se realice copia simultánea, medida de seguridad que ya ofrece la mayoría de los proveedores en Cloud.

- **Seguridad en el diseño *(Privacy by design)*.** Conscientes de la importancia de la seguridad de los datos a los que se tiene acceso a través de los servicios de GESTCARE iCLOUD, el proveedor deberá incluir medidas de seguridad integradas en el propio diseño de la aplicación.

  La introducción de este concepto en el ordenamiento jurídico español la encontramos en la Disposición adicional del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD), donde se establece la obligación de que los productos de software que traten datos de carácter personal automatizados incluyan en su descripción técnica el nivel de seguridad que se va a adoptar para los mismos.

  De igual modo, la previsión de la protección de datos desde el diseño también viene específicamente establecida en el artículo 25.3 en referencia al artículo 42 del recientemente aprobado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGLOPD) al introducir la promoción de mecanismos de certificación y sellos de calidad de los sistemas que contienen datos de carácter personal.

2.3.1. Servicios ofertados por GESTCARE iCLOUD

Como se ha hecho referencia con anterioridad, **los clientes a los que GESTCARE iCLOUD se dirige con la comercialización de su software en la nube son los propios Centros Médicos,** pero la utilización del mismo tiene una doble vertiente:

2.3.1.1. Software para la gestión médica por parte de las Clínicas y Centros Médicos.

Los servicios principales que GESTCARE iCLOUD oferta a las clínicas médicas y centros sanitarios son:

- **Gestión del HME del paciente.** Es la pieza básica que conforma la Historia Clínica del paciente. En la misma se incluirán tanto las notas de los facultativos sanitarios, como la documentación adjunta al mismo, como los análisis médicos, recetas y demás documentos que se incluyen en la Historia Clínica.
- **Gestión de las pruebas y análisis clínicos.** Registro del proceso de envío y recogida de los análisis clínicos al laboratorio, con la inclusión de los protocolos específicos para el tratamiento de los datos, su anonimización y demás procedimientos necesarios para el correcto tratamiento de los datos especialmente sensibles contenidos en los mismos. Idéntico procedimiento será realizado para el caso de otro tipo de pruebas médicas que el paciente requiera y que deban realizarse en diferentes centros y departamentos, ya sean internos, externos o adscritos al centro médico en cuestión.
- **Gestión administrativa del HME** en todo lo referente a los datos de contacto, citas, pagos y demás gestiones administrativas necesarias para poder llevar a cabo la asistencia sanitaria.
- **Soporte para la atención médica remota través de teléfono o webcam.** GESTCARE iCLOUD ofrece la aplicación para hacer posible tal asistencia. Se requiere consentimiento expreso del paciente para la prestación de asistencia médica en esta modalidad.
- **Atención médica integral 24h.** Con este servicio los pacientes pueden ser atendidos en cualquier lugar y a cualquier hora. Para ello, los mismos cuentan con un sistema de geolocalización en su dispositivo móvil a través del cual pueden ser localizados en cualquier lugar y en cualquier momento.

2.3.1.2. La gestión médica por parte de los propios pacientes.

A su vez, los pacientes cuentan con un perfil a través del cual acceden a través de su usuario y medidas de autenticación personal correspondiente. Los servicios a los que podrá acceder el paciente (dependiendo de los servicios contratados) son los siguientes:

- **Disponibilidad y acceso a su propio Historial Médico en todo momento,** incluidos diagnósticos, pruebas y análisis.
- Desde su cuenta de usuario el paciente podrá concertar citas, realizar pagos y todas las demás **gestiones administrativas** relativas a su Historia Clínica.
- **Soporte para la atención médica remota a través de teléfono o webcam.** Se requiere su consentimiento expreso para poder ser atendido en esta modalidad.
- **Atención médica integral 24h.** A través de este servicio, los pacientes pueden ser atendidos en cualquier lugar y a cualquier hora. Para ello, basta con que entren con su cuenta de usuario, previo consentimiento expreso a esta función, para que puedan ser geolocalizados en cualquier lugar y en cualquier momento y que de este modo, un médico o facultativo sanitario pueda atenderles allí donde se encuentren.

  A través de este servicio los pacientes pueden solicitar tanto asistencia remota como asistencia física en el lugar donde el paciente se encuentra, atendiendo a sus necesidades así como a las condiciones contractuales previamente establecidas.

3. **EL HISTORIAL MÉDICO ELECTRÓNICO EN LA NUBE**

3.1. ¿Qué es Historial Médico Electrónico (HME)?

Una primera definición del HME se encuentra en el Documento de Trabajo del Grupo de Trabajo del artículo 29 sobre Protección de datos, relativo a la salud en los historiales médicos electrónicos (HME), adoptado el 15 de Febrero de 2007, cuando configura el HME como *"un historial médico completo o una documentación similar del estado de salud física y mental pasado y presente de un individuo, en formato electrónico, que permita acceder fácilmente a estos datos a efectos de tratamientos médicos y otros fines estrechamente relacionados."*[2]

Asimismo, la Ley 41/2002 de 14 de Noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBAP), en una aproximación más exhausta, en su artículo 14.1 define la Historia clínica como "*el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro."* El mismo artículo en su apartado segundo también establece la obligación de que cada centro archive las historias clínicas de sus pacientes y que éstos son los responsables de garantizar su correcta seguridad, conservación y recuperación.

---

[2] *"Tratamientos médicos y otros fines estrechamente relacionados"* hace referencia al *"tratamiento de datos* (que) *resulte necesario para la prevención o para el diagnóstico médicos, de la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional"*, contenido en el apartado 3 del artículo 8 de la Directiva 95/46/CE relativa a la protección de datos de las personas físicas, derogada por el Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales, el cual establece en el artículo 9.2 h) y en el mismo sentido, indican que los datos sanitarios pueden ser tratados *" para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario"*

De este modo, el HME se configura como un elemento básico de información donde se concentran todos los datos de salud del paciente, incluyéndose en el mismo toda la información referente a su situación clínica pasada y presente, con la finalidad de disponer de un archivo personalizado en el que conste la información médica del paciente lo más exacta, veraz y actualizada posible y que de este modo pueda ser utilizada por los facultativos que atiendan al paciente, ofreciéndoles una asistencia y diagnóstico lo más acertada posible de acuerdo a sus necesidades. La normativa también establece la obligación de que los facultativos que acceden al mismo se identifiquen y que además los centros sanitarios sean los responsables del HME.

Finalmente, el paciente debe ser identificado con su nombre, apellidos y número de Historia Clínica, con la finalidad de ser identificable en el sistema de salud en el cual esté adscrito. Ahora bien, ¿qué tipo de dato es el dato de salud?

3.1.1. Dato sanitario como dato de carácter personal especialmente protegido

En primer lugar, es preceptivo determinar que **el dato sanitario es un dato de carácter personal,** y éste, a su vez, queda definido por el artículo 3 a) LOPD como "*cualquier información concerniente a personas físicas identificadas o identificables."* Pero además, el artículo 4.1) RGLOPD, amplía dicho concepto, determinando que serán datos personales "*toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."*

Por lo tanto, para que un dato sea considera como dato de carácter personal es necesario que sea un dato (1) concerniente a una persona física (2) identificada o identificable y además, la normativa europea extiende el concepto añadiendo que (3) la identidad pueda determinarse directa o indirectamente.

No cabe duda que los datos sanitarios cumplen estos tres requisitos, pues los datos sanitarios describen rasgos esenciales referentes a las personas físicas que les identifican o les pueden hacer identificables y además, los HME constan los datos de identificación del paciente, por lo que no cabe duda de que el dato de salud debe configurarse como un dato de carácter personal protegible por la legislación de protección de datos, tanto en cuanto a la normativa española establecida por la LOPD y desarrollada por el RDLOPD como por la normativa europea a través del Reglamento de Protección de Datos recientemente entrado en vigor.

El contenido del HME está formado, esencialmente, por datos de salud, razón por la cual, antes de adentrarnos es su nivel de protección y determinación de su tratamiento es preceptivo establecer una definición del mismo.

Para ello debemos acudir al artículo 5.1. g) RDLOPD cuando determina que serán "*datos de carácter personal relacionados con la salud:* ***las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo***.[3] *En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética."*

Los datos sanitaros son datos especialmente protegible los cuales sólo serán tratados bajo determinadas excepciones, las cuales serán referidas en el apartado 3.7.

3.1.2. Principios aplicables al HME

Para que los datos personales puedan ser recogidos, tratados y almacenados automáticamente en el HME, deben cumplirse los principios los siguientes[4]:

[3] Asimismo, está definición de dato sanitario también viene recogida en el Considerando 45 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (en adelante, Convenio 108 del Consejo de Europa).

[4] Principios contenidos en los artículos 5 RGPD, 4 LOPD y 8 RDLOPD

- Principio de calidad de los datos. Este principio exige que los datos tratados sean los necesarios para cumplir con el fin concreto para el que fueron recogidos. Es decir, que estos datos sean pertinentes y no se excedan respecto al fin concreto con el que se pretende cumplir. Además, también se exige que los mismos sean exactos y estén actualizados. Por lo tanto, el HME solamente debería contener aquellos datos que sean necesarios para la asistencia médica del paciente.[5]

- Principio de limitación de uso. En relación con el principio de calidad de los datos, no está permitido un tratamiento posterior de los datos de carácter personal con una finalidad que sea incompatible con aquella para la que fueron recogidos. Por consiguiente, **los datos recogidos para la asistencia médica del paciente, no podrán ser tratados para otros fines sin el consentimiento del paciente.**

- Principio de acceso del interesado. Los interesados podrán acceder en cualquier momento al HME para verificar la exactitud de los datos contenidos en él y asegurarse de que están actualizados en todo momento.

- Principio de retención de los datos, según el cual los datos personales deberán retenerse como máximo, durante el tiempo necesario para el fin que se recabaron, almacenado o tratado. En el caso del HME, los datos que conforman la Historia Clínica del paciente son recabados durante todo el tiempo que dure la asistencia sanitaria e incluso después, si el paciente desea conservar su HME.

- Seguridad de los datos: Principios de integridad, confidencialidad y disponibilidad de los datos. Para garantizar la seguridad de los datos contenido en el HME, es necesario que estén disponibles todos los datos que contienen el HME (integridad), que pueda disponerse de ellos en cualquier momento en que sea necesario (disponibilidad), y que además, solamente accedan aquellas personas que estén autorizadas en las condiciones y términos necesarios para el tratamiento, de acuerdo a su fin.

[5] En este sentido, en artículo 15.4 LBAP dispone que *"la historia clínica se llevará con criterios de unidad y de integración".*

Para ello, el responsable del tratamiento debe aplicar medida técnicas, organizativas y de controles tendientes a garantizar que se cumplen las obligaciones de seguridad que protejan los datos de carácter personal de intromisiones indebidas.

Este punto es especialmente importante en el caso que nos ocupa, ya que, debido a que los datos son tratados por varios agentes, en diferentes localizaciones y a través de internet, se hace necesario el estricto establecimiento de todas las medidas de control necesarias para evitar accesos inconsentidos.

3.1.3. Contenido básico del HME

El HME debe incluir todos los datos necesarios para la correcta asistencia y diagnóstico médico del paciente así como todos los procesos asistenciales, ya sean respecto a la atención primaria o especializada del paciente. Concretamente, el artículo 15 LBAP establece que el contenido mínimo de la historia clínica, independientemente del soporte en el que se encuentre, incluirá:

- El consentimiento explícito e informado del paciente o de sus representantes legales, sin el cual y como regla general, no es posible el tratamiento de sus datos personales.
- Las órdenes médicas que se deben llevar a cabo para una correcta asistencia.
- La documentación relativa a la hoja clínicoestadística.
- La autorización de ingreso, siempre y cuando el paciente sea capaz de darla, de acuerdo a sus circunstancias.
- El informe de urgencia, que debe incorporarse a su HME.
- La exploración física y diagnóstico médico, incluidas las anotaciones subjetivas del facultativo médico.
- Los informes de exploraciones complementarias.

- La evolución médica del paciente.
- La hoja de interconsulta siempre que el paciente sea atendido por más de un facultativo médico, por ejemplo, cuando un mismo paciente es tratado por más de un especialista.
- El informe de anestesia en el que el paciente debe prestar consentimiento expreso y por escrito, después de que se le haya informado de los riesgos que ello implica.
- El informe de anatomía patológica.
- La evolución y planificación de cuidados de enfermería.
- La aplicación terapéutica de enfermería.
- El gráfico de constantes.
- El informe clínico de alta autorizado por el facultativo médico correspondiente una vez haya finalizado en proceso asistencial y de acuerdo con los artículos 20 y 21 LBAP. Como regla general, el paciente podrá firmar su alta voluntaria en todo momento, y en virtud de su autodeterminación como paciente.

Además, por razón de los servicios prestados por este proveedor, el HME que éste oferte también deberá contener:

- Las pruebas biométricas, médicas o analíticas que se realicen al paciente.
- Registro y copia de recetas y prescripciones farmacológicas o de otra índole emitidas por el médico al paciente por razón de sus asistencia médica.
- Contratos y documentación que acredite la prestación de los servicios sanitarios al paciente por parte del centro sanitario concreto, así como los datos económicos, el estado de sus pagos y demás datos económicos y de gestión administrativa y de los recursos.
- Los documentos relativos al consentimiento expreso a la asistencia remota y geolocalización, en caso de haber contratado estos servicios.

- La identificación del paciente por el medio que él determine como medio preferente de acreditación (DNI, nombre y apellidos, código de registro…).

En conclusión, el software en la nube ofertado por GESTCARE iCLOUD ofrece a sus clientes todas la aplicaciones que permiten la inclusión de estos elementos dentro de cada uno de los HME de los pacientes que son tratado en el seno de las consultas o centros médicos en los que son atendidos.

Finalmente, el programa de gestión contiene herramientas que permiten desarrollar nuevas aplicaciones de acuerdo a las necesidades concretas de cada clínica.

3.1.4. Derechos de información y consentimiento del paciente

En primer lugar, en materia de Protección de Datos, se establece como derecho genérico de los titulares de los derechos personales el ser informado *"de manera expresa, precisa e inequívoca"*, de que va a ser recogidos y tratados, tal y como lo recoge el artículo 5 LOPD.

Esta obligación corresponde al responsables del tratamiento de los datos del HME, quienes deben comunicarle la información básica al interesado acerca del tratamiento de los datos contenidos en él así como los fines a los que se destina dicho tratamiento, los destinatarios de los mismo, la posibilidad de ejercer los derechos de acceso, rectificación y cancelación y oposición ante el responsable del tratamiento (derechos ARCO), si existen derechos de acceso por parte de terceros, de qué modo y a qué datos se va a acceder.

Este hecho es distinto al derecho a la derecho a la información asistencial que contiene la LBAP en virtud del cual los pacientes tienen derecho de ser informados sobre cualquier actuación que concierna a su salud –y el derecho que los mismos tienen a no serlo-, la cual, se realizará, como norma general, de forma verbal y contendrá como mínimo, la finalidad, la naturaleza de su asistencia, los riesgos y consecuencias. Esta información se comunicará

a los pacientes de una manera comprensible y de acuerdo a su situación concreta por el médico y los demás profesionales que le presten asistencia.[6]

Por lo tanto, debemos distinguir entre el derecho que los pacientes tienen a ser informados respecto de su asistencia médica, en virtud de su **autonomía como paciente**; del consentimiento que deben prestar los mismos para tratar sus datos personales, el cual ser prestado de manera expresa y por escrito. Este es un buen ejemplo de cómo la transversalidad de la normativa en materia de protección de datos debe armonizarse con la normativa sectorial sanitaria y de autonomía del paciente.

Pero, ¿quién debe ser informado de estos hechos?

Además de las garantías de las que se le dota al paciente como titular de los datos de carácter personal contenidos en el HME, la LBAP le coloca como titular del derecho a información contenida en el mismos, así como a todas las personas que estén vinculadas a él y a las que, de manera expresa o tácita, les hubiera habilitado para tal fin.

En caso de incapacidad, cuando las capacidades en las que se encuentre el paciente no permitan una normal comprensión de su estado de salud, debe ser informado de la manera más comprensible posible de acuerdo a su estado y en todo caso, se informará a sus representantes legales o a las personas vinculadas a él y que le acompañen en el momento de la asistencia. El único límite referente al derecho de información es el caso de que, por necesidad terapéutica, el facultativo médico determine que tal información puede perjudicar gravemente la salud del paciente, en cuyo se debe dejar constancia en el Historial Clínico y se informará a los familiares o personas vinculadas al paciente.[7]

Pero, no es suficiente con que el paciente sea informado sino que además debe prestar su consentimiento informado, libre, voluntario e inequívoco. Es decir, sin que quepa ninguna duda de que el paciente conoce y consiente que sus datos sean recabados, almacenados y tratados, tal y como establecen tanto el artículo 6 LOPD como el artículo 8 LBAP.

[6] Art. 4 LBAP.

El consentimiento verbal dejando constancia en el HME es la regla general en la asistencia sanitaria, pero se requiere la prestación del consentimiento por escrito en los casos de aplicación de procedimientos más complejos y graves en los que se ponga en riesgo la vida del paciente o supongan inconvenientes de notoria y previsible repercusión negativa sobre su salud, como pueden ser el suministro de anestesia, una intervención quirúrgica, procedimientos diagnósticos u otros tratamientos terapéuticos invasores.[8]

Sin embargo, no será necesaria la prestación de dicho consentimiento cuando exista riesgo para la salud pública por razones sanitarias establecidas por ley[9] y cuando el tratamiento de estos datos tenga como finalidad proteger el interés vital del interesado, siempre y cuando no se vulneren sus derechos y libertades[10].

Los derechos de información y consentimiento deben constar expresamente en las condiciones y Términos de Uso de los Servicios de GESTCARE iCLOUD y asimismo, también deben ser tenidos en cuenta para la implantación de medidas técnicas de aseguramiento y control que permitan el cumplimiento de estas obligaciones por parte de las clínicas y centros médicos que contraten sus servicios con este proveedor de servicios.

---

[7] Art. 5 LBAP

[8] Según el artículo 10, en los casos en los que se necesite el consentimiento por escrito, debido a la gravedad y los riesgos en la salud y la propia vida del paciente, el facultativo deberá informar al paciente de:

"a) Las consecuencias relevantes o de importancia que la intervención origina con seguridad.

b) Los riesgos relacionados con las circunstancias personales o profesionales del paciente.

c) Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención.

d) Las contraindicaciones."

[9] Art. 9.2.a) LBAP.

[10] Art. 6.2 LOPD Y ART. 9.2. b) LBAP.

3.2. Identificación y registro de los pacientes y demás sujetos que acceden al HME[11]

El HME gestionado por GESTCARE iCLOUD ofrece a sus clientes diferentes perfiles a través de los cuales tanto el paciente como el personal del centro podrán acceder a las partes del mismo a las que estén autorizados en virtud de rol que tomen respecto a la asistencia del paciente, así como el consentimiento prestado por el mismo, de acorde a la legislación vigente en la materia. Para ello, tanto el paciente como los demás actores deben seguir el procedimiento que se muestra a continuación, según el cual se deberán reunir unas medidas de seguridad determinadas de acuerdo, tanto del sujeto que se trate como, sobre todo, el nivel de protección de los datos contenidos en él. En consecuencia, se proponen las medidas siguientes:

3.2.1. Identificación de los pacientes

Es muy importante que los pacientes de los que se recaben los datos para almacenarlos en el HME estén debidamente identificados en el sistema informático de gestión médica. Para ello, es de vital importancia que esta identificación sea fiable, en el sentido de que esté garantizado que los datos que se contienen en el HME coincidan con la identidad del sujeto.

El registro debe hacerse por parte del propio usuario prestando su consentimiento al médico o facultativo que le asista. Posteriormente, se requiere la confirmación del consentimiento prestado, validando los datos correspondientes desde su perfil, una vez haya sido dado de alta en el sistema como usuario del centro médico. Para tal validación, los pasos que el paciente debe llevar a cabo son los siguientes:

[11] El procedimiento de identificación se ha configurado en relación a las medidas de seguridad que se exponen en el apartado "3.7. Medidas de Seguridad".

- El paciente adquiere una clave pública facilitada por GESTCARE iCLOUD en una tarjeta de coordenadas, junto con una contraseña formada por cuatro dígitos que podrá modificar a su criterio y en cualquier momento.
- Posteriormente, el paciente se identifica con su nombre y apellidos, DNI/pasaporte y fecha de nacimiento. También es posible la identificación a través de firma electrónica avanzada y compatible con el sistema de GESTCARE iCLOUD.
- El paciente introducirá su clave privada (que ha podido ser modificada por el usuario respecto de la facilitada en el centro médico) y además, se le pedirá uno de los dígitos incluidos en la tarjeta de coordenadas.
- Al acceder al sistema, el paciente debe validar el consentimiento prestado en la clínica o centro sanitario. Este consentimiento se llevará a cabo una sola vez y con el objetivo en poner en marcha el HME (sin perjuicio del consentimiento que el mismo debe prestar para los casos específicos anteriormente prestados).
- Cada vez que el paciente acceda al sistema, le aparecerá un cuadro de diálogo avisándole de que a través de este acceso está consintiendo que los dato sean recabados y tratados de acuerdo al artículo 7.6 LOPD, con un enlace direccionado a la web en la que puede acceder a lo término y condiciones de uso.

Los pacientes deben ser mayores de 18 años para contratar los servicios de GESTCARE iCLOUD por primera vez. En lo restante, se seguirán las directrices establecidas en el apartado 3.3.1.3., referente al acceso de los pacientes menores de edad.

Siguiendo estas directrices, los pacientes podrán acceder a su HME a través de internet con independencia horaria y de localización, e incluso descargarse en su dispositivo las partes del HME de las que precise, siempre y cuando se respeten los derechos de terceros.[12]

3.2.2. Identificación de los médicos y demás facultativos sanitarios

Al igual que los pacientes, los médicos y facultativos sanitarios deben estar identificados de una manera fiable y según la cual pueda validarse su identidad como individuo así como profesional facultativo autorizado para el acceso a la parte del HME correspondiente. Para registrarse en el sistema, el facultativo sanitario debe:

- Registrarse mediante firma electrónica avanzada emitida por el colegio de abogados correspondiente. Éste también será el sistema elegido para su identificación y acceso al sistema.

  Una vez dado de alta en el sistema, dispone de un perfil personal como facultativo médico desde el cual accederá al HME del paciente.

2.3.3. Identificación del personal administrativo

Debido a que los datos a los que va a acceder el personal administrativo son aquellos que solo requieren medidas de protección baja (datos de contacto, facturas y gestión de las citas), la identificación del personal administrativo se lleva a cabo a través de usuario y contraseña.

El usuario corresponde a un número de identificación corporativa en el sistema y la contraseña debe estar compuesta por 8 dígitos y la obligatoria combinación de números y letras en mayúsculas y minúsculas. La contraseña debe cambiarse con una periodicidad de, como mínimo, una vez al mes.

[12] La cuestión acerca del acceso al HME queda resuelta en el apartado 3.3 del presente Informe.

3.3. El acceso al Historial Médico Electrónico

3.3.1. Tipos de acceso

El HME es accesible por diferentes actores que participan en él, pero no todos tienen acceso a las mismas partes de la Historia Clínica. A continuación se detallan tanto quienes pueden acceder al HME, como el modo y el alcance de los accesos.

3.3.1.1. El acceso al HME por parte del propio paciente

El paciente, como titular del HME, tiene derecho a acceder al mismo en cualquier momento, tanto por ser titular de los datos contenidos como por el derecho que le concede la autonomía del paciente a ser informado y prestar consentimiento respecto de todos los procesos asistenciales que se lleven a cabo en referencia a su propia salud, vida e integridad física y psíquica.

El acceso según la normativa en materia de protección de datos

Como regla general, el paciente debe saber que como titular de los datos sanitarios contenidos en el HME, puede ejercitar los derechos que le otorga la normativa referente a la protección de datos.

De este modo, existe un Registro General de Protección de datos en el cual deben inscribirse todos los ficheros que contienen datos de carácter personal. El mismo es público y gratuito y a él pueden acudir los titulares de estos datos para conocer la existencia de tratamiento de los mismos, sus finalidades y la identificación del responsable del tratamiento. No es posible, sin embargo, conocer la identidad de las demás personas que traten los datos, siempre que se sitúen en la esfera del responsable.[13] También debe informársele de las correspondientes cesiones de datos así como de la posibilidad de ejercitar sus derechos de acceso, rectificación y cancelación (derechos ARCO), facultades de las que se les dota a los titulares de los datos para que puedan ejercer un control efectivo

[13] Art. 14 LOPD.

de los mismos. En concreto, nos interesa el derecho de acceso, contenido en el artículo 15 LOPD y desarrollado en los artículos 27 a 30 del RDLOPD.

La solicitud de acceso debe dirigirse directamente al centro sanitario - responsable del fichero- donde constan los datos, el cual debe resolver la solicitud en el plazo máximo de un mes desde la recepción de la misma. En caso contrario, el titular de este derecho puede acudir a la Autoridad de Protección de Datos – La Agencia Española de Protección de Datos- para que sus derechos sean tutelados. Si la solicitud es favorable, el acceso debe hacerse efectivo durante los diez días siguientes.

Es importante destacar que el derecho de acceso a los datos personales contenido en la LOPD sólo puede ser ejercitado en intervalos no inferiores a 12 meses, salvo que exista una acreditación de interés legítimo que faculte al interesado para que pueda reducir estos plazos. Este derecho es personalísimo pero puede ejercitarse por su representante legal en caso de incapacidad así como un representante voluntario, cuando el interesado así lo haya designado voluntariamente.

Finalmente, cabe indicar la posibilidad de que, en virtud del artículo 26 RDLOPD, el paciente pueda ejercitar sus derechos ARCO ante GESTCARE iCLOUD, como encargado del tratamiento, para que éste dé traslado de la petición al responsable del tratamiento, es decir, al Centro Sanitario. La regla general es que el paciente ejerza sus derechos ante el centro médico, ya que es el actor con el que éste se relacionará, pero es menester en este informe, indicar que existe esta posibilidad.

Estas reglas de acceso pueden resultar muy rígidas al tratarse de datos especialmente sensibles y que se refieren a derechos tan básicos como la propia salud de las personas, la integridad física y moral e incluso la propia vida. Es por ello que el acceso al HME se encuentra regulado con más detalle en la normativa sectorial sanitaria y en concreto, en la Ley Básica de Autonomía del Paciente.

<u>El acceso según la normativa específica sanitaria</u>

La LBAP reconoce específicamente en su artículo 18 el derecho que tienen los pacientes al acceso a la documentación clínica y a obtener copia de los datos que constan en ella. Por lo tanto, en el caso del HME, este acceso se produce cuando el paciente se identifica y autentica electrónicamente en el sistema, a través del cual accede a su HME de manera segura, impidiendo el acceso de terceros. Este derecho también puede ejercerse a través de representación, o cuando prestando su consentimiento, el titular consienta ceder sus claves de acceso a terceras personas.

El acceso desde el perfil del paciente le concede a éste la facultad de leer la información contenida en el HME, tanto en lo referente su diagnóstico como a las pruebas en él adjuntas (siempre y cuando no se vulneren derechos de terceros). Asimismo, puede descargar dicha información en su dispositivo Electrónico seguro, quedando además registrada la fecha y hora desde la que se realiza la descarga.

3.3.1.2. El acceso al HME por un tercero distinto al paciente

La regla general es que el Historial Médico, como fichero que contiene datos personales del paciente, no es accesible por terceros sin su consentimiento. Por este motivo, el principio general es que solamente tendrán acceso él y los profesionales que por razón de sus funciones estén habilitados para tal fin, dentro del ámbito de actuación del centro que sea responsable del fichero en el que están contenidos los datos. De este modo, el artículo 7 de la LBAP al establecer que *"toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley"*. Por lo tanto, lo que quiere proteger este precepto es el derecho a la intimidad del que gozan los pacientes, dentro del derecho a su propia autodeterminación, limitando expresamente el acceso de terceros.

Sin embargo, como se ha indicado en el apartado 3.1.4. referente al consentimiento, esta misma ley habilita la posibilidad de que las personas vinculadas a él por razones familiares o de hecho puedan acceder a la información asistencial del paciente, que normalmente se lleva a cabo en el momento de la asistencia médica y de forma verbal. También es posible

que un tercero acceda con el consentimiento o por representación del paciente. Fuera de estos casos, **el acceso por parte de terceros a HME está prohibido.**

Caso distinto es cuando el paciente haya fallecido. En este supuesto, los familiares o personas vinculadas a él pueden acceder al mismo - salvo que éste lo haya prohibido expresamente- cuando exista un riesgo para su salud, en cuyo caso el acceso se limitará únicamente a aquellos datos necesarios para mitigar este riesgo.

Asimismo, el derecho a la intimidad no se pierde con el fallecimiento, motivo por el cual el familiar o persona que ostente una situación similar de vinculación con el paciente, no puede afectar con su acceso la intimidad del titular del HME a las anotaciones efectuadas por el médico ni los derechos de terceros, en caso de que los hubiera.[14]

3.3.1.3. Acceso al HME del menor

En primer lugar, el derecho a la protección de datos es un derecho personalísimo, por lo que debe estar ejercido por el propio menor siempre que sea mayor de 14 años y no exista inhabilitación legal para ello. En este caso, la información dirigida a ellos debe ser adecuada y comprensible de acuerdo a su edad. Para ello, deben llevarse a cabo los procedimientos necesarios para garantizar este derecho, como son las comprobaciones de edad y la autenticidad de su consentimiento. En el caso de ser menores de 14 años, debe prestarse el consentimiento de los padres o tutores. (artículo 13 RDLOPD).

En el ámbito sanitario, el artículo 5 LBA en referencia al derecho a la información asistencial, abre la posibilidad de que el paciente sea representado por los familiares o personas vinculadas a él de hecho **en caso de que carezca de capacidad suficiente física o psíquica para ser informado de su situación clínica**. Éste es el caso de los menores, los cuales verán su capacidad modulada respecto a su edad y madurez.

[14] Art. 18.4 LBAP

Por lo tanto, establecidas las premisas legales, la problemática está en hacer confluir el derecho a la intimidad, la confidencialidad y protección de datos del menor con el derecho de información de los padres que ostenta la patria potestad de sus hijos.

Aunque la LOPD habilita a los mayores 14 años para el ejercicio de los derechos de carácter personal de los que él es titular, en lo que se refiere a los datos de carácter sanitario , la LBAP establece que:

- Los menores emancipados o mayores de 16 años, como regla general, tiene la capacidad suficiente para prestar su consentimiento informado[15] y asimismo, también pueden ejercer sus derechos de acceso, siempre y cuando no estén incapacitados judicialmente o sean capaces intelectual y emocionalmente para entender el alcance de su asistencia o intervención. A partir de esta edad se le reconoce una esfera íntima en la que el mismo es titular de estos derechos personalísimos, pudiéndolos ejercer contra otros, incluidos sus familiares o personas vinculadas a él.

  Sin embargo, en caso de enfermedad grave y en caso de que no exista autorización del menor en contrario, será posible que los padres o tutores puedan acceder al HME. También deben ser tenidas en cuenta las legislaciones específicas en cuanto a la interrupción voluntaria del embarazo o los tratamientos de reproducción asistida, en las que la edad exigida para la representación del menor puede ser modulada.

- Entre los 12 y 16 años es necesario escuchar la opinión del menor teniendo en cuanta su capacidad intelectual y emocional., aunque el consentimiento corresponde a los padres.

- En cuanto a los menores de 12 años se presume que no son capaces ni intelectual ni emocionalmente para prestar conocimiento, por lo que sus derechos se ejercitan a través de sus padres o tutores, sin perjuicio de que, debido a la relevancia que tienen

[15] Art. 9.4 LBAP.

los datos relativos a su salud, ellos sean informados de acuerdo a su capacidad de comprensión.

Por consiguiente, el alta en el sistema, identificación, registros y derechos de acceso en el sistema, se dará conforme a estas previsiones legales.

3.3.1.4. El acceso al HME por parte de médico titular

En la evolución del paciente es esencial el acceso del médico que le presta asistencia sanitaria (artículo 16.1 LBAP), así que éste se configura como el actor principal que va a participar en el mismo a través de la elaboración de los diagnósticos y demás anotaciones, dentro del ámbito del responsable del HME, de acuerdo a la finalidad perseguida –la asistencia sanitaria-. Sin embargo, el acceso al HME por parte del médico no es un acceso ilimitado sino que únicamente puede acceder a las partes del HME necesarias para la consecución de tal fin. Es así como queda determinado en el artículo 18.3 LBAP.

Esto es especialmente relevante cuando en el mismo HME se gestiona la asistencia de diferentes médicos especialistas, de modo que el médico que presta la asistencia primaria no tiene por qué acceder a la información sobre la asistencia por el especialista de traumatología o cualquier otro.

De este modo, se garantiza la confidencialidad de la asistencia médica y el respeto a la intimidad tanto del paciente como del médico que lo elabora, en especial a las anotaciones subjetivas creadas por el mismo. Es por ello que se requiere un control de accesos para cada uno de estos facultativos. Ahora bien, estos accesos deben ser dinámicos y configurarse desde una visión integral, de modo que en caso de que médico requiera de la información y documentación elaborada por otro médico, pueda obtenerla sin grandes dificultades, siempre que se requiera para prestar asistencia médica al paciente dentro de su ámbito de actuación y sin que pueda excederse de la información que sea requerida para tal fin.

3.3.1.5. El acceso al HME por parte del médico de urgencias

Como se ha establecido con anterioridad, GESTCARE iCLOUD ofrece un servicio de Asistencia 24h a través del cual, el usuario puede ser atendido en cualquier momento y en cualquier lugar. Esta asistencia es llevada a cabo por un médico de urgencias que esté de guardia en aquel momento.

Aunque no sea el médico titular al que el paciente esté asignado, éste también está habilitado legalmente para acceder al HME del paciente con el fin de llevar a cabo cualquier asistencia de urgencia que sea requerida por el paciente.

La figura de médico de guardia debe estar de alta y tener un perfil específico en el sistema (con independencia de que el médico que realiza estas funciones tenga otro perfil como médico de cabecera o médico especialista).

En el ejercicio de estas funciones, el médico sólo puede acceder al HME con motivo de la asistencia sanitaria concreta, y en el sistema de la propia HME quedará registrado este acceso con las correspondientes anotaciones, evaluaciones y diagnósticos del médico de urgencias, así como las pruebas y recetas aportadas por el mismo, quedando constancia de la fecha y hora en la que se produce este acceso. De este modo, el paciente puede consultar el registro sobre los accesos llevados a cabo por los diferentes médicos en la asistencia de urgencia.

En todo caso, siempre quedará constancia (1) de que el acceso ha sido realizado por razón de urgencia, (2) la identificación del médico que accede, (3) la causa concreta que justifica el acceso y a qué parte del HME se accede, (4) la hora y fecha del acceso y (5) el lugar donde se ha llevado a cabo la atención de urgencia o si, en su caso, ha sido de manera remota.

3.3.1.6. Acceso al HME por parte del personal de enfermería

El artículo 16.1 establece que podrán acceder al HME los profesionales asistenciales que los requieran *"como instrumento fundamental para su correcta asistencia"*.

El personal de enfermería tiene condición de profesional asistencial sanitario de acuerdo con la Ley 44/2003, de 21 de noviembre, de Profesiones Sanitarias, así que estos

facultativos podrán acceder al HME para la finalidad necesaria para el desarrollo de su actividad profesional, siempre y cuando se respete en principio de proporcionalidad y exactitud de acuerdo a cada caso concreto[16] y que deberá aplicarse de forma restrictiva.

La base de la necesaria aplicación del juicio de proporcionalidad la encontramos en el respecto a la intimidad del paciente, la confidencialidad entre médico y paciente y la privacidad del médico en cuanto a las anotaciones subjetivas que éste escribe en el HME, necesarias para el correcto diagnóstico del paciente.

Para llevar a cabo estas tareas, se habilita un perfil de enfermero a través del cual solo es posible el acceso al HME cuando es validado por un facultativo médico. Debido a que el facultativo enfermero puede acceder a más de una parte del HME por motivo del fin de su asistencia sanitaria, la autorización médica es un buen mecanismo de control de sus actividades. Esta autorización no es necesaria que se dé en cada caso concreto, pudiéndose hacer de manera general, atendiendo siempre al caso concreto.

Asimismo, al inicio de la prestación de los servicios, el paciente debe prestar consentimiento explícito al acceso del personal de enfermería a su HME.

3.3.1.7. El acceso al HME por parte del personal de Administración

El HME además de la propia historia clínica del paciente, también está formado por todos los datos que hacen posible que la asistencia sanitaria se lleve a cabo, como son los datos de contacto, el registro de las citas, admisiones del paciente, presupuestos, etc. Así, el HME además de la función de asistencia médica también tiene como finalidad la **gestión** de la misma. Es por ello que el artículo 16.4 LBAP habilita al personal de Administración para acceder a aquellos datos referidos a la gestión.

[16] Así lo determina el Informe 656/2008 AEPD referente al Acceso a la Historia Clínica de sus pacientes por parte del personal sanitario de los centros, en particular cuando se trata del personal de enfermería que desempeña su puesto de trabajo en hospitalización y que necesariamente debe acceder a la historia clínica para llevar a cabo la adecuada asistencia sanitaria de los pacientes.

Para estas funciones, el personal de administración cuenta con un perfil específico para estas funciones y el nivel de seguridad para el acceso a los mismos es menor que a los perfiles que acceden a datos sanitarios, atendiendo a datos contenidos en esta parte del HME.

3.3.1.8. El acceso al HME para las funciones de inspección, evaluación, acreditación y planificación.

El acceso a la Historia Clínica del paciente para estas funciones también tiene su previsión legal en el artículo 18 LBAP. De este modo y en virtud del principio de calidad, los inspectores sanitarios pueden acceder a las Historias Clínicas con la función de supervisar el correcto funcionamiento de los actores que participan en el mismo y retirarlas si no cumple con la normativa ni los principios referentes en esta materia.

Asimismo, siguiendo el artículo 124.2 del Decreto 2065/1974, de 30 de mayo por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social *"los inspectores y farmacéuticos del Cuerpo de Inspección Sanitaria de la Administración de la Seguridad Social tendrán la consideración de autoridad pública en el desempaño de tal función y recibirán de las autoridades y de sus agentes la colaboración y del auxilio que a ella se deben´´*. Si esta inspección se realiza a una historia clínica centralizada, se entenderá que este acceso es un acceso legítimo en virtud del principio de calidad. Sin embargo, si la historia clínica es descentralizada, estaremos ante una cesión de datos habilitada por la Ley, y por lo tanto, ante la que no se requiere consentimiento del interesado.[17]

[17] De acuerdo al Documento de Trabajo del Grupo de Trabajo del artículo 29 sobre Protección de datos, relativo a la salud en los historiales médicos electrónicos (HME), adoptado el 15 de Febrero de 2007(pág.18) entiende como HME de almacenamiento centralizado: *"el HME como un sistema uniforme de almacenamiento, al que los profesionales médicos deben transferir su documentación"* y como almacenamiento descentralizado *"el HME como sistema que proporciona acceso a los historiales médicos que guarda el profesional de salud, que tiene la obligación de conservar un historial sobre el tratamiento de sus pacientes".*

Es menester señalar que el almacenamiento en los sistemas de GESTCARE iCLOUD se lleva a cabo de manera centralizada, pues es garantía de mayor disponibilidad y seguridad técnica al sistema, notas muy importantes y definitorias de este proveedor de servicios en la nube.

3.3.4. Revocación del acceso por parte del paciente

En virtud, tanto de la posibilidad que tiene el titular de los datos de carácter personal de ejercitar sus derechos ARCO, como de los derechos reconocidos por LBAP en cuanto a su autonomía como paciente, éste puede revocar su consentimiento a los permisos otorgados a todos o alguno de los actores que acceden a su HME, así como la posibilidad de retirar su HME del sistema de la clínica en la que se encuentra. En este sentido, es muy importante la interoperabilidad del sistema informático con el que se opera, pues de ello dependerá que los datos contenidos en el HME que gestiona GESTCARE iCLOUD puedan seguir siendo tratados por otras clínicas que utilicen un programa de gestión diferente.

En el momento en el que el paciente revoque el consentimiento a un facultativo concreto para el acceso al HME, el mismo:

- No podrá consultar el HME ni los datos contenidos en el mismo. Es decir, se le denegará el acceso al HME concreto.

Y en caso de ser médico, además el mismo no podrá:

- Introducir nuevas anotaciones en el HME del paciente ni consultar las que él mismo haya hecho hasta el momento.

3.3.5. Límites al acceso

El derecho de acceso del paciente a la Historia Clínica puede verse limitado en dos casos[18]:

- Cuando con el acceso del paciente se produzca un perjuicio a terceras personas, justificado por la confidencialidad de los datos que constan en ella en interés terapéutico del paciente.

  Este es el caso del familiar o un tercero que para ayudar al facultativo sanitario en su asistencia médica al paciente revela información que no quiere que sea conocida por el paciente en lo que se refiere a algunos hechos, datos o a su identidad. Con la protección de la confidencialidad y el derecho a la intimidad de estas terceras personas lo que se pretende es que el miedo de este tercero a la revelación de los datos que ha facilitados no ponga en peligro la salud o la vida del paciente.

- Para la protección la intimidad y libre desarrollo de la actividad profesional de los facultativos médicos, los cuales pueden oponerse a que el paciente accedan a sus anotaciones subjetivas. En este caso, n este caso, será posible el acceso al diagnóstico asistencial pero en los casos que el médico lo considere oportuno, éste podrá oponerse a que el interesado acceda a las notas subjetivas. La aplicación de este límite deberá ejercitarse utilizando el principio de proporcionalidad y en todo caso, cuando la oposición del facultativo médico no impida al paciente conocer su estado de salud.[19]

---

[18] Art. 18.3 LBAP

[19] . En este sentido, la Resolución de la AEPD R/00969/2008, de 31 de Julio de 2008 se pronuncia del siguiente modo:

"Los datos personales de la interesada que deben ser facilitados en atención al derecho de acceso, son todos aquellos datos relativos a la determinación y constatación de sus lesiones, su evolución y, en su caso, las secuelas advertidas, que afectan a la salud de la titular de los datos, pero no pueden incluirse, como datos de base, las valoraciones o apreciaciones de índole médica sobre el encaje de las lesiones o secuelas padecidas en la aplicación del baremo del Real Decreto Legislativo 8/2004 que deben ser consideradas estimaciones de orden técnico propias de un facultativo médico.

Como consecuencia, el informe que especifique los días empleados en la curación, su efecto impeditivo o no, así como la concreta puntuación de las secuelas subsistentes una vez alcanzada la estabilización lesional, excede en lo aplicable al derecho de acceso, por lo que no es competencia de la Agencia Española de Protección de Datos."

3.4. El tratamiento de datos sanitarios

3.4.1. ¿Qué requisitos deben cumplirse para el tratamiento de estos datos?

Tal y como se indicó en el apartado 3.1.1., el dato sanitario es un dato personal especialmente protegido. Es por ello que la regla general en la normativa de protección de datos, es que esta tipología de datos no puede ser tratada.[20]

Sin embargo, tanto las normas supranacionales como la misma LOPD[21] que este tipo de datos pueden ser tratados cuando:

a) El interesado consienta expresamente. Este consentimiento constituye la norma general.

b) El tratamiento se lleve a cabo por razones de interés general.

c) Así se establezca legalmente.

d) Dicho tratamiento sea necesario para la prevención o diagnóstico en el marco de la asistencia sanitaria, realizándose en todo momento por un profesional sanitario sujeto al secreto profesional. Es decir, este supuesto se dará cuando el paciente no esté en condiciones de poder prestar su consentimiento y siempre y cuando sean tratados los datos necesarios para la consecución de tal fin.

e) Para salvaguardar el interés vital del paciente o de un tercero, siempre que el paciente esté en una situación de incapacidad de hecho o de derecho y no pueda prestar su consentimiento.

[20] Es así lo que señala el art. 6 del Convenio 108 del Consejo Europa cuando establece la prohibición de tratamiento automatizado de los datos de carácter personal referentes al origen racial, opiniones políticas, convicciones religiosas, aquellos relativos a la salud o a la vida sexual, a los cuales el Reglamento 2016/679 de Protección de Datos en su art. 9.1 añade las convicciones filosóficas, la afiliación sindical, los datos biométricos y genéticos destinados a la identificación de una persona.

En cuanto al ordenamiento interno español, en el art. 7 de la LOPD se establecen idénticas directrices para el tratamiento de este tipo de datos.

[21] Art. 7.3 y 7.6 LOPD, así como los art. 9.2 a), c),g), h) y el art. 9.4 RGLOPD.

Asimismo, el artículo 8 LOPD indica que serán las instituciones y centros médicos – tanto públicos como privados- así como los profesionales correspondientes dentro de los mismos, quienes podrán tratar los datos de carácter personal relativos a la salud, de acuerdo a la normativa específica sanitaria.[22]

Por lo tanto, sabemos que los datos sanitarios pueden ser tratados cuando se dé uno de estos tres supuestos pero, ¿qué se entiende por tratamiento de datos de carácter personal?

El artículo 3 d) LOPD y el artículo 5.1 t) RDLOPD comparten definición al establecer 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."*

En consecuencia, estas operaciones y procedimientos se llevan a cabo respecto a los datos de carácter personal, y en especial, los datos sanitarios contenidos en el HME siempre que se dé uno de los requisitos establecidos anteriormente y este tratamiento se realice para uno de los fines por los que el mismo se justificó.

Cabe apuntar además, que no deben tratarse otros datos que los que sean estrictamente necesarios para la consecución de los fines en los que se justifica. Los sujetos que intervengan en el HME deben tener especial cuidado a la hora de introducir otros datos diferentes a los médicos, máxime cuando puedan ser también datos especialmente protegidos referentes a su religión, creencias, etc. Así, por ejemplo, en el HME no deberían contenerse datos de pertenencia a una determinada religión en caso de que el paciente no consienta hacerse transfusiones de sangre.

3.4.2. ¿Qué sujetos intervienen?

[22] Normativa específica sectorial a la cual se hace referencia apartado relativo a la cesión de datos.

Los principales sujetos que intervienen en el tratamiento de los datos personales son:

- El centro médico en calidad de cliente y responsable del tratamiento de los datos personales.
- GESTCARE iCLOUD como proveedor de los servicios y encargado del tratamiento de los datos personales.
- Los demás sujetos que tratan los datos personales como subencargados del tratamiento dentro del ámbito del encargado del tratamiento.

El cliente que contrata los servicios de gestión en la nube, como responsable del tratamiento de los datos, debe hacerlo con la mayor diligencia posible, garantizando siempre que se cumplan los principios básicos en cuanto a los datos personales de los cuales es responsable (art. 20.2 RDLOPD). Este deber de diligencia también alcanza a la diligencia de contratar con un proveedor que garantice que en caso de subcontratar los servicios de encargado del tratamiento, los datos van a seguir estando a salvo.

3.4.2.1. Responsable del tratamiento

El responsable del tratamiento es aquella "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo,* ***que decida sobre la finalidad, contenido y uso del tratamiento.***"[23]

Así, en virtud esta facultad de decisión que tiene el responsable del tratamiento sobre el tratamiento de los datos, puede tratarlos él directamente o puede elegir que otro realice el tratamiento en su nombre bajo las directrices que éste le indique.

Este es el caso del cliente que decide contratar los servicios que GESTCARE iCLOUD ofrece en la nube para la gestión del HME de sus pacientes ya que es el primero quien

[23] Art. 3 d) LOPD.

decide cómo van a ser tratados los datos contenidos en el mismo – de forma externa por el proveedor- determinando así la finalidad y los usos que se le van a dar a este tratamiento.

Además, el responsable tiene la obligación de establecer las medidas técnicas y organizativas necesarias para la protección de los datos personales contenido en el HME, el encargado de obtener la autorización y el consentimiento de los pacientes para el tratamiento de sus datos personales, ante quién se puede ejercer los derechos ARCO y en, definitiva, tiene la obligación de velar por los datos personales contenidos en los ficheros de los que es responsable. Estas obligaciones no pueden ser alteradas contractualmente, ya que son imperativos legales.

Por su parte, la LBAP identifica a los centros sanitarios como los obligados a facilitar el acceso de los pacientes a sus historias clínicas (artículo 18.4) y a custodiar las Historias Clínicas de los pacientes del propio centro (artículo 19).

De este modo, no cabe ninguna duda de en el caso del HME, **son los centros médicos los que ostentan la posición de responsables del tratamiento** de los datos personales incluidos en él.

3.4.2.2. Encargado de tratamiento

El encargado del tratamiento es aquél que trata los datos de acuerdo a los fines, directrices y por cuenta del responsable. Por lo tanto, **el proveedor de servicios en la nube GESTCARE iCLOUD es el encargado del tratamiento de los datos contenidos en el HME** ya que es quien suministra la plataforma y los medios técnicos para llevar a cabo este fin, que será determinado por el centro médico concreto.

El proveedor de servicios también está obligado a establecer las medidas técnicas y organizativas para la seguridad de los datos que trata, a la confidencialidad, a asistir y cooperar con el responsable del tratamiento en la asistencia de éste en el ejercicio de los derechos ARCO de los interesados.

En caso de que el encargado del tratamiento utilice estos datos para fines distintos a los señalados por el responsable del tratamiento o los comunique a terceros fuera del ámbito

organizativo de éste, el encargado del tratamiento será considerado también responsable y de este modo responderá por las infracciones en las que por ello hubiera incurrido.[24]

Para determinar la relación entre responsable y encargado del tratamiento, debe suscribirse un contrato entre responsable y encargado del tratamiento en el que se establezca explícitamente los términos y condiciones del tratamiento. [25]

Finalmente, cuando el encargado del tratamiento haya cumplido con la prestación establecida contractualmente por ambas partes, los datos de carácter personal que haya estado tratando durante la misma han de ser destruidos o devueltos en las mismas condiciones en los que fueron facilitados.

3.4.2.3. Subencargado de tratamiento

Debido a la propia estructura y configuración de los servicios de Cloud Computing, es muy habitual que el tratamiento de datos que corre a cuenta del encargado del tratamiento (proveedor) a su vez, se lleve a cabo por otros encargados del tratamiento (subencargados del tratamiento) en el que éste se apoya para prestar sus servicios.

La normativa en materia de protección de datos abre la posibilidad de que el proveedor del servicio en la nube delegue en terceros parte sus tareas a través de la subcontratación, siempre y cuando exista autorización por parte del responsable del tratamiento.

Para ello, deben seguirse las siguientes directrices[26]:

a) Que en el contrato de prestación de servicios entre responsable y encargado del tratamiento se especifique la posibilidad de subcontratar los servicios con terceros así como la identificación de estos terceros subcontratados.

[24] Artículo 2. RDLOPD.

[25] Anexo 2: Contratos de prestación de servicios de Cloud Computing

[26] Art. 21 RDLOPD.

En caso de no haber terceros subcontratados en el momento de la celebración del contrato, se le comunicará al responsable los datos de identificación de este tercero antes de proceder a la subcontratación. Aunque no existan terceros subcontratados, se podrá establecer en el contrato entre cliente y proveedor el tipo de servicios que va a poder ser subcontratados o unos mínimos estándares de calidad.

b) Que el tratamiento de los datos por parte del subcontratista se haga de acuerdo a las directrices pactadas entre responsable y encargado del tratamiento.

c) Que los términos y condiciones en los que el subcontratista preste sus servicios por cuenta del encargado del tratamiento queden específicamente establecidas en un contrato suscrito entre ambas partes.

d) En caso de que el subcontratista no cumpla con sus obligaciones en materia de protección de datos, el encargado del tratamiento responderá por ello ante el responsable. Esta premisa constituye una garantía de diligencia del encargado del tratamiento ante el responsable del tratamiento, sobre todo cuando los datos están tratados en terceros países que no cuentan con un nivel de protección adecuado.

3.5. Cesión de datos

La regla general para el tratamiento de datos de carácter personal es el necesario consentimiento del titular de los mismos[27], quien debe autorizar al responsable del tratamiento para que los trate de acuerdo al determinado fin para el cual fue designado. También existe la posibilidad de que estos datos sean tratados por terceros pero solo en la medida en la que estén designados por el responsable del tratamiento para el fin que éste le ha delimitado (son los casos del encargado y subencargado del tratamiento). Fuera de estos supuestos, la comunicación a terceros de datos personales con otros fines distintos a aquél consentido por el interesado constituye un supuesto de cesión de datos.[28]

Pese a ello, existen casos en los cuales no se precisa de consentimiento del paciente para que los datos de carácter personal sean cedidos a terceros. De acuerdo los artículos 16.3 LBAP así como los artículos 7.6 y 11.2 LOPD, cobran especial relevancia:

- Cesión para fines epidemiológicos, de salud pública y de investigación.
- Cesión de la historia clínica a la administración sanitaria
- Cesión a las compañías aseguradoras
- Cesión a las fuerzas y cuerpos de seguridad del Estado.
- Cesión a los órganos judiciales

Fuera de estos supuestos en los que prima el interés general, las comunicaciones de datos a terceros sin el consentimiento del interesado y fuera del ámbito de aplicación del responsable del tratamiento, serán ilícitas

[27] En el caso de datos de salud además, el consentimiento debe prestarse por escrito y de manera expresa.

[28] Art. 11.1 LOPD.

3.6. Transferencias Internacionales de datos

3.6.1. Regla general: Transferencias Internacionales a países que no proporcionan un nivel de seguridad equiparable

Una de las características principales en los servicios en Cloud es que la prestación de los mismos puede llevarse a cabo en diferentes lugares sin que el cliente tenga conocimiento exacto de dónde están sus datos.

Aunque desde un punto de vista técnico, en principio, ello no suponga grandes dificultades. No podemos decir lo mismo en lo referente a la protección de los datos que se tratan en la prestación de estos servicios, pues no todos los países tienen el mismo nivel de protección.

Para delimitar el ámbito de aplicación de esta comunicación de datos debemos acudir al artículo 5.1 s) RDLOPD en el que se definen las trasferencias internacionales de datos como el *"Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español."*

Asimismo, deben identificarse las figuras de:

- Exportador de datos como el sujeto que, situado en el territorio español, realiza la TI a un sujeto situado un Estado fuera de la EEE (art. 5.1. j) RDLOPD).
- Importador de datos como el sujeto situado fuera del EEE que recepciona los datos emitidos desde el territorio español (art. 5.1. ñ) RDLOPD).

Por lo tanto, nos encontramos ante un supuesto de Transferencias Internacionales (TI) cuando (1) exista una transmisión de datos fuera del Espacio Económico Europeo por parte del exportador de datos y (2) sin importar que el importador de estos datos los recepcione en virtud de una cesión de datos como de un tratamiento de datos realizado bajo la

responsabilidad de un responsable del tratamiento establecido dentro del Espacio Económico Europeo, delimitado por las normas europeas en materia de protección de datos.

Este puede ser el caso de un proveedor Cloud que opera en el EEE pero que almacena los datos físicamente, por ejemplo, en un servidor en la India. Las TI de datos son muy habituales porque los costes económicos son más bajos en fuera del territorio de la Unión Europea.

En caso de que existan TI, el para poder exportar datos a países terceros, es necesaria la autorización AEPD (art. 33.1 LOPD) excepto en los casos que se refieren en el art. 34 LOPD.

Esta facultad puede llevarse a cabo mediante **Cláusulas Contractuales Tipo (CCT)** aprobadas tanto por la Comisión Europea como por la AEPD.[29]

Asimismo, las Reglas Corporativas Vinculantes (RCV) permiten la transferencia de datos a países terceros siempre que los datos se transfieran dentro de empresas del mismos grupo empresarial siguiendo las prerrogativas del artículo 70.4 RDLOPD.

3.6.2. Excepciones

3.6.2.1. Nivel equiparable o adecuado de protección

El artículo 35.1 LOPD indica, asimismo, la posibilidad de que se puedan tratar datos de carácter personal en países que proporcionen un nivel adecuado de protección, llamado también "Puerto Seguro (o Safe Harbour)" aunque se trate de un país fuera de la EEE. [30]

[29] "*Consultas más frecuentes (FAQS). Garantías a aportar cuando el servicio de Cloud Computing implique una transferencia internacional de datos que necesite la autorización de la AEPDE"* 5 de Noviembre de 2015 https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00005

Problemática de las transferencias internacionales de datos con Estados Unidos: Anulación del Puerto Seguro (Safe Harbour)

Especialmente importante es el caso de EEUU, donde además de ser un país que España cuenta con muchos lazos comerciales, también es el lugar donde se sitúan muchas operaciones relacionadas con el tratamiento de datos en la nube.

Hasta el pasado 6 de Octubre, éste era un país con un nivel de protección adecuado pero fue desde el famoso caso de la Sentencia del Tribunal de Justicia de la Unión Europea en el Caso Schrems[31], cuando este tribunal consideró que las comunicaciones de datos al país Americano vulneraban los derechos fundamentales de la vida privada y familiar (artículo 7 CDFU) y el derecho a la protección de datos de carácter personal (artículo 8 CDFUE).[32]

Es por ello que a partir de entonces, EEUU ya no constituye un país con un adecuado nivel de protección para la comunicación de datos y ya no se hacen de acuerdo al derecho europeo sino que deberán seguirse las normas de las TI.

3.6.3. Propuesta para GESTCARE iCLOUD en materia de Transferencias Internacionales de datos

El establecimiento de un nivel adecuando de protección de los datos de carácter personal supone la garantía de que estos datos que van a ser tratados por terceros diferentes al titular de los mismos sean protegidos.

---

[30] Anexo 1: Lista de los países declarados con un nivel adecuado de protección.

[31]

Es por ello que, desde esta parte, la propuesta para GESTCARE iCLOUD es que, a su vez, intente, en la medida de lo posible, que los proveedores de los que se sirva para la prestación de los servicios estén ubicados en el EEE.

Este proveedor de servicios debe ser consciente de la importancia de que todos los componentes estén ubicados tanto es EEE o en un territorio de equivalente protección, tanto en lo que se refiere a la subcontratación de los servicios de subcontratación del tratamiento como de las infraestructuras físicas donde se almacenan los datos.

Ello facilitará la prestación del servicio y dará confianza a los clientes que contraten con el servicio en la nube para la gestión médica ya que, debido a que se tratan datos muy delicados referentes a la salud y propia vida del paciente, éstos van a tener muy en cuenta el lugar donde sus datos personales van a ser tratados.

3.7. Medidas de seguridad[33]

Como hemos ido viendo a lo largo de todo este informe, no son pocos los riesgos a los que los datos de carácter personal se ven sometidos desde su recogida y tratamiento hasta su almacenamiento en todos los puntos y por todos los sujetos que van a ser tratados. Pero, ¿a qué nos referimos exactamente cuando hablamos de medidas de seguridad?

El artículo 9 LOPD define como medidas de seguridad las *"medidas de índole técnica y organizativa necesarias para que se garantice la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural"*. Y es así como se pronuncia el artículo 17 LBAP cuando establece que *"los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad".*

Por lo tanto, no cabe duda que el responsable del tratamiento de los datos personales está obligado a velar por el establecimiento y cumplimiento de estas medidas. En este caso, el centro médico.[34]

Finalmente, cabe establecer que para el cumplimiento de las medidas de seguridad, es necesario que se respete el principio de seguridad de los datos, formado asimismo, por los principios de integridad, disponibilidad y confidencialidad.[35]

3.7.1. El documento de seguridad

[33] Los procesos de identificación contenidos en el apartado 3.2 han sido elaborados de acuerdo a las medidas de seguridad contenidas en el presente apartado.

[34] Art.14.2 LBAP

[35] Tal y como se ha indicado con anterioridad en el apartado "3.1.2. Principios aplicables al HME" de este mismo documento.

El responsable del tratamiento de los datos debe elaborar un documento en el que se contemplen todas las medidas técnicas y organizativas tendientes a garantizar la seguridad de los datos sujetos a su responsabilidad. Este documento es el denominado documento de seguridad[36].

El documento de seguridad es de obligado cumplimiento para todos aquellos sujetos que tengan acceso a los sistemas de información donde estén contenidos los datos personales y además se le dota de la categoría de documento interno dentro de la organización.

En cuanto a la forma, puede existir un solo documento que incluya todos los ficheros o bien uno individualizado para cada fichero o tratamiento organizado, por ejemplo, según el nivel de protección de los datos u otros criterios dentro del ámbito de organización del responsable y, en todo caso, debe contener, como mínimo, los aspectos introducidos en el artículo 88.3 RDLOPD[37].

Adicionalmente, y puesto que los ficheros referentes a los HME tratan datos de nivel alto, se deben incluir dos datos más: la identidad del responsable así como los controles periódicos tendientes a verificar el cumplimento de las medidas contenidas en el mismo documento.[38]

---

[36] Art. 88 RDLOPD.

[37] *Art. 88.3 a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.*

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos."

El documento de seguridad debe ser adaptado a las particularidades de cada clínica o centro médico, de acuerdo a sus necesidades y su modo de organización de los recursos.

3.7.2. Nivel de seguridad para los datos contenidos en el HME

Los artículos 89 a 104 RDLOPD establecen las medidas de seguridad que deben implementarse para garantizar el correcto acceso y tratamiento a los datos, eliminando las posibles vulneraciones de los titulares de los mismos, ya se deba a un mal uso de los mismos o a un acceso inconsentido.

Estas medidas se gradúan en tres niveles (bajo, medio y alto) dependiendo de la naturaleza de los datos y siguiendo las reglas del artículo 81 RDLOPD.

Específicamente, y en cuanto a lo que respecta al HME, el artículo 81.3 RDLOPD establece que a los datos de salud se les aplicarán medidas de nivel alto.

Además, el proveedor, dentro de su oferta comercial, presta el servicio de Asistencia Integral en el cual se utiliza la geolocalización móvil. Éste dato también debe estar protegido con medidas de seguridad de nivel alto, como así lo estipula el art. 81.4 RDLOPD.

Por otro lado, los datos referentes a la gestión administrativa del HME cuenta con un nivel de protección bajo. Es por ello que la opción más acertada respecto a la implementación de las medidas de seguridad y de acceso a los datos contenidos en el HME, es hacerlo de manera separada (en el mismo sentido al establecido en el apartado 3.2 respecto a la Identificación y registro de los pacientes) y de acuerdo a los distintos perfiles con los que cuentan cada uno de los profesionales que interviene en el sistema.

Las concretas medidas de seguridad que todos los datos contenidos en el HME (tanto los de contacto como las de carácter sanitario) deben contener son:

[38] Art. 88.4 RDLOPD.

- Establecimiento de perfiles de usuario claramente identificados en el documento de seguridad (art. 89 RDLOPD).
- Registro de incidencias (art. 90 RDLOPD).
- Control de accesos (art. 91 RDLOPD).
- Posibilidad de gestión de los soportes de manera que sea posible identificar la información contenida en ellos y el registro del destino que se les va a dar: traslados, salida, procedimientos de destrucción o borrado y demás procedimientos que se lleven a cabo deben estar contenidos en el documento de seguridad. Deben ser supervisados por el responsable del tratamiento, quien debe controlar que se realice correctamente.
- Identificación y autenticación de los usuarios que acceden a los datos personales. Cuando la autenticación consiste en una contraseña (como, en este caso, ocurre en los ficheros de los datos a los que accede el personal administrativo), deberá incluirse en el documento de seguridad la periodicidad en la que las mismas deben ser cambiadas. Para el caso concreto de GESTCARE iCLOUD, debe llevarse a cabo con una periodicidad de, como mínimo, una vez al mes.

Asimismo, los datos de nivel medio deben contener las siguientes medidas de seguridad:

- Designación de un Responsable de Seguridad, para uno o más ficheros. Los datos de identificación del mismo así como de su ámbito de responsabilidad deben constar en el documento de seguridad.
- Informe de auditoría bienal.
- Gestión y soporte de documentos, estableciendo un registro de entradas y salidas en el que también se pueda indicar la fecha y hora, destinatario y otros datos de identificación y registro. Los perfiles ofertados por este proveedor permiten, ya desde el diseño, el registro de estos datos.
- Registro de incidencias

Y, finalmente, se añaden las siguientes medidas de nivel alto:

- Realización de copias de seguridad. En cuanto a los datos de nivel alto, el RDLOPD obliga a que se realicen, al menos, una vez por semana. Sin embargo, es aconsejable la copia simultánea, debido a que en relación con las características técnicas de los servicios en la nube, se puede conseguir una disponibilidad prácticamente total por un coste muy asequible.
- El registro de accesos tal y como se establece en el apartado dedicado a la identificación.
- Obligación del cifrado en la transmisión de los datos a través de vías de telecomunicación.

Por lo tanto, como los datos de nivel alto deben contener las medidas de seguridad de todos los otros niveles, para proteger los datos sanitarios, las clínicas y centros médicos que contraten los servicios deben establecer todas las medidas hasta ahora establecidas, a las que el proveedor de servicios debe prestarle soporte técnico.

Adicionalmente, es muy importante que en los centros se elaboren protocolos o códigos de buenas prácticas para los usos de los sistemas de información, ya que muchas veces las vulneraciones o intromisiones ilícitas vienen dadas por el mal uso que les da el personal interno de la propia organización.

Una buena aplicación de las Medidas de Seguridad en los sistemas electrónicos que dan acceso a datos personales, lejos de hacerlos más vulnerable, refuerza la seguridad de los mismos, además de hacerlos más disponibles y actualizados, pudiendo además tener un control exhaustivo de los accesos que se hagan al HME.

4. CONCLUSIONES

Como bien indica el título del presente informe, el objeto del mismo ha sido determinar las implicaciones jurídicas que conlleva la puesta en marcha del prestador de servicios de gestión en la nube GESTCARE iCLOUD para establecer relaciones comerciales con clínicas y centros médicos situados en el estado español.

Es cierto que, en un principio, los servicios de Cloud Computing llevan aparejados muchos riesgos de seguridad debido, sobre todo, a la deslocalización de los datos y los diferentes agentes que intervienen en la recolección, tratamiento y almacenamientos de los mismos, motivo por el cual han sido presentadas indicaciones y propuestas para que el uso de estos servicios se haga de modo seguro, máxime cuando se trata de datos tan sensibles como los datos referentes a la salud.

Especial atención caben las referencias al HME y sus implicaciones en cuanto a los accesos y tratamiento de los datos, confluyendo, de este modo, la normativa tanto nacional como internacional en materia de protección de datos, así como la normativa sectorial relativa a la propia autonomía que tiene el paciente en virtud de su autodeterminación personal.

Finalmente, todas las implicaciones jurídicas entre GESTCARE iCLOUD y la clínica con la que contrate quedan plasmadas en el contrato de servicios adjuntan en el Anexo 2, actuando de este modo, como fuente de derecho entre las partes.

Después de analizar todas estas cuestiones, no cabe más que concluir con la determinación de que existen riesgos en materia de protección de datos pero que con la diligencia adecuada y de acuerdo con las propuestas realizadas a lo largo de todo el informe, es totalmente posible y viable jurídicamente la prestación de servicios en la nube para la gestión médica (en concreto, la gestión del Historial Médico Electrónico) en las clínicas y centros médicos establecidos en el territorio español.

5. BIBLIOGRAFÍA

Libros

- ✓ MARTÍNEZ MARTÍNEZ, Ricard. Enero, 2014. *Derecho y Cloud Computing.* Monografías. Pamplona: Thomson Reuters, CIVITAS, ISBN: 978-84-470-3852-7.

Revistas

- ✓ ÁLVAREZ HERNANDO, Javier. *Acceso a datos por cuenta de terceros. El encargado del tratamiento y su régimen jurídico. Servicios de «cloud computing»*. Enero, 2014. Grandes Tratados. Practicum Protección de Datos 2015. Editorial Aranzadi, SA. ISBN 978-84-9059-821-4.
- ✓ DÍAZ DÍAZ, Efrén. *El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones.*2016. Revista Aranzadi Doctrinal num.6/2016 parte Estudio. Editorial Aranzadi, S.A.
- ✓ GUASCH PORTAS, Vicente. *Cloud Computing, cláusulas contractuales y reglas corporativas vinculantes*. Ibiza, 2014. Revista de Derecho UNED, núm 14. pp 247-269.
- ✓ JOYANES AGUILAR, Luis. 2012. *Computación en la nube. Notas para una estrategia española en cloud*. Revista del Instituto Español de Estudios Estratégico núm. 0/2012.pp. 89-112.
- ✓ PINEDO GARCÍA, Igor. Protección de datos sanitarios: *la Historia Clínica y sus accesos.* Revista CESCO de Derecho de Consumo nº8/2013. pp. 306-318.
- ✓ MORALES, José Ramón, 2013. *Cloud Computing: riesgos corporativos e implicaciones jurídicas.* Pamplona, Editorial Aranzadi, SA. Actualidad Jurídica Aranzadi num.863/2013.

- ✓ OPPENHEIM Charles. *Legislación sobre computación en la nube y negociación en los contratos.* Septiembre-Octubre 2012. El profesional de la información v.21, n.5. ISSN: 1386-6710.
- ✓ RENGIFO GARCÍA, Ernesto. *Computación en la nube*. Noviembre de 2013. México, Revista de la Propiedad Inmaterial nº17. pp.223-245.
- ✓ TRONCOSO REIGADA, Antonio. *La confidencialidad de la historia clínica.* Enero-Abril 2006. Cuaderno de Derecho Público, núm. 27. pp- 45-143.

Tesis

- ✓ TORRES i VIÑALS, Jordi. *Del Cloud Computing al Big Data. Visión introductoria para jóvenes emprendedores.* Barcelona, Universitat Oberta de Catalunya.

Artículos en línea

- ✓ KUAN HON, H, MILLARD Christopher, WALDEN, Ian. 2012. *Negotiation Cloud Contracts: Looking at clouds from both sides now*. Stanford, Stanford Technology Law Review Volume 16, Number 1 Fall 2012. Disponible en: http://stlr.stanford.edu/pdf/cloudcontracts.pdf
- ✓ NIST, Mell, P. y Grance, T.: *The NIST Definition of Cloud Computing*, 2011, p. 2 Disponible en http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Guías

- ✓ AEPD. *Orientaciones para prestadores de servicios de Cloud Computing.* 2013.
- ✓ AEPD. *Guía para clientes que contraten servicios de Cloud Computing.* 2013.

- ✓ AEPD. *Guía del responsable de ficheros.* NIPO: 052-08-001-5.
- ✓ OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN. *Guía para empresas: Seguridad y privacidad del cloud computing.* 2011. INTECO

Dictámenes del Grupo del artículo 29

- ✓ Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos. (MHE). 15 de febrero de 2007.
- ✓ Dictamen 4/2007 de 20 de Junio sobre el concepto de dato personal.
- ✓ Dictamen 1/2010 de 16 de Febrero de 2010 sobre los conceptos de responsable y encargado del tratamiento.
- ✓ Dictamen 05/2012 de 1 de Junio de 2012 sobre la computación en nube.

Legislación

- ✓ CONVENIO 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984
- ✓ Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- ✓ Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- ✓ Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- ✓ Ley 41/2002 de 14 de Noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica
- ✓ Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.
- ✓ Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Recursos web

- ✓ *Consultas más frecuentes (FAQS). Garantías a aportar cuando el servicio de Cloud Computing implique una transferencia internacional de datos que necesite la autorización de la AEPDE.* 5 de Noviembre de 2015. AEPD. https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/detallePreguntaFAQ.jsf?idPregunta=FAQ%2F00005
- ✓ *Países con un nivel adecuado de protección.* AEPD. Disponible en línea en: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php
- ✓ www.agpd.es
- ✓ aranzadi.es
- ✓ elderecho.com
- ✓ http://ec.europa.eu/justice/data-protection/

Informes y Resoluciones AEPD

- ✓ Informe 656/2008 referente al acceso a la historia clínica por parte del personal de enfermería. Gabinete Jurídico. AEPD
- ✓ Resolución R/00969/2008, de 31 de Julio de 2008. AEPD.

Jurisprudencia

- ✓ Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) Caso Maximillian Schrems contra Data Protección Commissioner. TJCE 2015\324

ANEXOS

Anexo 1: Lista de los países declarados con un nivel adecuado de protección.

"Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes:

- ***Suiza.*** *Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000*
- ***Canadá.*** *Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos*
- ***Argentina****. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003*
- ***Guernsey****. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003*
- ***Isla de Man.*** *Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004*
- ***Jersey.*** *Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008*
- ***Islas Feroe.*** *Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010*
- ***Andorra.*** *Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010*
- ***Israel.*** *Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011*
- ***Uruguay.*** *Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012*
- ***Nueva Zelanda.*** *Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012"*

Fuente: *Países con un nivel adecuado de protección.* AEPD. Disponible en línea en: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

Anexo 2. ***Modelo de contrato de Cloud Computing en lo que respecta al tratamiento de datos personales***[39]

En _____, a ___ de ____de 20____

REUNIDOS

I. De una parte, la sociedad AMIGOS, S.A., de nacionalidad española, con domicilio social en Calle _____ de _____ y con C.I.F. A-_____ (en adelante, el RESPONSABLE DEL TRATAMIENTO). Se halla representada por D. _____, con N.I.F. _____, respectivamente, quien actúa en calidad de _____.

II. De otra parte, la entidad GESTCARE iCLOUD, S.L., con domicilio social en _____, con C.I.F. _____ (en adelante, EL ENCARGADO DEL TRATAMIENTO). Se halla representada por D. _____, con N.I.F. _____, respectivamente, quien actúa en calidad de _____.

EXPONEN

I. Que el RESPONSABLE DEL TRATAMIENTO es titular de dos ficheros que contienen datos de carácter personal denominados CLIENTES POTENCIALES y CLIENTES, correctamente inscritos en el Registro General de Protección de Datos (los «Ficheros»). El Fichero CLIENTES POTENCIALES contiene datos relativos a nombre, apellidos, dirección y teléfono, y el Fichero CLIENTES contiene datos relativos a nombre, apellidos, dirección y teléfono, cuentas corrientes, y servicios contratados (los «Datos Personales»).

[39] Fuente: ÁLVAREZ HERNANDO, Javier. *Acceso a datos por cuenta de terceros. El encargado del tratamiento y su régimen jurídico. Servicios de «cloud computing»*. Enero, 2014. Grandes Tratados. Practicum Protección de Datos 2015. Editorial Aranzadi, SA. ISBN 978-84-9059-821-4. pp. 40-47.

II. Que el ENCARGADO DEL TRATAMIENTO y el RESPONSABLE DEL TRATAMIENTO han suscrito un Contrato, con fecha ... de ... de ..., en virtud del cual el ENCARGADO DEL TRATAMIENTO prestará ciertos servicios al RESPONSABLE DEL TRATAMIENTO, conllevando dicha prestación de servicios la realización de un tratamiento de datos personales, a través de un servicio de computación en nube (cloud computing).

III. Que el **ENCARGADO DEL TRATAMIENTO y el RESPONSABLE DEL TRATAMIENTO están interesados en establecer el marco contractual que regule los servicios de cloud computing** , conforme a lo previsto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos personales (LOPD) y los artículos 20 y siguiente del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD).

IV. Que, por tanto, con el objeto de ofrecer garantías suficientes respecto de la protección de la vida privada y de los derechos y libertades fundamentales de las personas respecto a los tratamientos de sus datos de carácter personal, en los servicios de cloud computing, ambas Partes, reconociéndose la capacidad legal necesaria, convienen en la celebración del **presente CONTRATO DE PRESTACIÓN DE SERVICIOS DE COMPUTACIÓN EN NUBE (el «CONTRATO»),** que se regirá de acuerdo con las siguientes

CLÁUSULAS

1. TRATAMIENTO DE DATOS POR CUENTA DE TERCEROS.

Ambas partes declaran que el servicio implica un el tratamiento de datos por cuenta de terceros, de manera que el cliente de los servicios de cloud computing _____ será considerado como responsable del tratamiento ya que decide sobre la finalidad, contenido y uso del tratamiento en cualquiera de sus formas. Por su parte, el prestador del servicio.

adquirirá el carácter de encargado del tratamiento no pudiendo, en modo alguno, decidir sobre el contenido, finalidad y uso del tratamiento y siempre que su actividad no le reporte otro beneficio que el derivado de albergar los datos, sin utilizarlos en modo alguno en su provecho, ya que en ese caso sería considerado igualmente como responsable del tratamiento.

2. DETERMINACIÓN DE LA LEY APLICABLE.

La ley aplicable será la de _____ es decir, la española, como responsable del tratamiento/cliente del servicio de computación en nube, salvo lo relativo a medidas de seguridad si el prestador se ubica en otro Estado Miembro de la UE.

3. SERVICIOS OBJETO DE LA PRESTACIÓN.

El tipo de servicio de computación en nube objeto de la prestación es el considerado de **«Software como servicio (SaaS)»,** ofreciendo el ENCARGADO DEL TRATAMIENTO los recursos básicos y el usuario o RESPONSABLE DEL TRATAMIENTO controla el sistema operativo y determinados componentes de red, como, por ejemplo, firewalls o cortafuegos. En ese caso el ENCARGADO DEL TRATAMIENTO proporciona capacidades de almacenamiento y proceso en bruto, sobre las que RESPONSABLE DEL TRATAMIENTO ha de construir las aplicaciones que necesita su organización. Se proporciona capacidad de almacenamiento masivo a través de la red y servidores de alojamiento web.

Por su parte, la modalidad de Cloud Computing es el considerado como «Nube privada», por lo que el RESPONSABLE DEL TRATAMIENTO realiza la gestión y administración de sus servicios en la nube, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella.

Detalles técnicos del servicio objeto de prestación: _____

4. RESPONSABILIDAD DEL ENCARGADO DEL TRATAMIENTO.

EL ENCARGADO DEL TRATAMIENTO se compromete a prestar los SERVICIOS observando, en todo caso, el procedimiento que se ajuste a las instrucciones que en cada momento indique EL RESPONSABLE DEL TRATAMIENTO, así como lo dispuesto en la normativa legal aplicable, no estando autorizada la utilización de dichos datos con un fin distinto al establecido en el cuerpo del presente contrato.

EL ENCARGADO DEL TRATAMIENTO se obliga a no realizar ningún otro tratamiento distinto del solicitado por EL RESPONSABLE DEL TRATAMIENTO, de los datos a los que tenga acceso, comprometiéndose, además, a no hacer uso de los Ficheros en su propio beneficio o en el de un tercero.

El Encargado del Tratamiento será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el Encargado del Tratamiento responderá de las infracciones en que hubiera incurrido personalmente.

El Encargado del Tratamiento indemnizará al Responsable del Fichero por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato. A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El Encargado del Tratamiento, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

La responsabilidad del Encargado del Tratamiento incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el Responsable del Fichero, como resultado del incumplimiento del Encargado del Tratamiento de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del Responsable del

Fichero en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

5. MEDIDAS DE SEGURIDAD

El ENCARGADO DEL TRATAMIENTO está obligado a implementar las medidas de seguridad correspondientes al nivel básico –a la vista de la naturaleza de los datos a los que está autorizado a acceder– según se regula en los artículos 9 de la LOPD y 79 y siguientes del RLOPD.

A continuación se detallan las concretas medidas de seguridad a implementar, por parte del encargado del tratamiento:

1) Se exige la aplicación de técnicas robustas de cifrado tanto a los datos en tránsito como a los datos almacenados.

2) _____

El RESPONSABLE DEL TRATAMIENTO debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable, para lo cual el ENCARGADO DEL TRATAMIENTO permitirá realizar las comprobaciones encaminadas a tal fin.

El ENCARGADO DEL TRATAMIENTO debe haber realizado una auditoría externa e independiente, sin importar el nivel de seguridad que sea de aplicación, respecto al cumplimiento normativo de las medidas de seguridad correspondientes atendiendo a lo establecido en el RLOPD. A tal fin, el ENCARGADO DEL TRATAMIENTO debe aportar una copia del INFORME DE AUDITORÍA resultante de la misma al RESPONSABLE DEL TRATAMIENTO.

El RESPONSABLE DEL TRATAMIENTO debe ser informado diligentemente y de forma inmediata, y por escrito, por parte del ENCARGADO DEL TRATAMIENTO, y en su caso, por el subencargado aceptado, sobre las incidencias de seguridad que afecten a los datos de

los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse.

6. ESTÁNDARES E INDICADORES DE CALIDAD DEL SERVICIO. ACUERDO DE NIVEL DE SERVICIO.

El ENCARGADO DEL TRATAMIENTO acredita en este momento, mediante copia justificativa, que dispone de una certificación que acredite su SGSI (Sistema de Gestión de la Seguridad) y su SGCN (Sistema de Gestión de Continuidad del Negocio), al igual que resulta condición para los posibles subencargados del tratamiento de cloud computing.

La renovación periódica de dichas certificaciones deben de ser comunicadas de forma inmediata al RESPONSABLE DEL TRATAMIENTO, al igual que debe entregarse copia del informe resultante de la auditoría, siendo causa de resolución del contrato su omisión.

Acuerdo de nivel de servicio: (...)

NOTA: En este apartado se pueden especificar los indicadores de calidad de servicio que van a ser medidos y los valores mínimos aceptables de los mismos.

7. COPIAS DE SEGURIDAD DE LOS DATOS

El ENCARGADO DEL TRATAMIENTO se compromete a asegurar la disponibilidad permanente e integridad de la información, objeto del servicio, para lo cual procederá a realizar copias de seguridad de los datos a fin de asegurar su pérdida accidental o provocada. En este caso, los datos no se deberán almacenar en una única ubicación, obligándose además el ENCARGADO DEL TRATAMIENTO a conservar una copia de seguridad fuera de línea.

Cada una de las copias o reproducciones estará sometida a los mismos compromisos y obligaciones que en este documento se establecen.

8. UBICACIÓN DE LOS RECURSOS

Los recursos técnicos sobre los que se sustenta el servicio de Cloud Computing, incluyendo las copias de seguridad, objeto del presente contrato se ubicarán SIEMPRE en territorio del Espacio Económico Europeo (países de la Unión Europea e Islandia, Liechtenstein y Noruega), por lo que no se considera que exista una transferencia internacional de datos (TID).

9. DISPONIBILIDAD DEL SERVICIO Y COMPENSACIONES POR INTERRUPCIÓN

En el supuesto de que el servicio, objeto del presente contrato, se vea interrumpido por la causa que fuera, dentro del horario de __ h a __ h y de ___ h a ___ h, por tiempo superior a 1 hora, haya preaviso o no, ello dará derecho al RESPONSABLE DEL FICHERO a exigir una compensación que consistirá en una rebaja del precio estipulado en el contrato principal de cloud computing que consistirá en _____.

Si la interrupción del servicio fuera superior a 5 horas, dentro del horario anteriormente citado, ello dará derecho al RESPONSABLE DEL TRATAMIENTO a cancelar el contrato principal de cloud computing, así como a percibir los daños y perjuicios que pudieran ocasionarse, debidamente cuantificados por una entidad auditora independiente.

En el supuesto de que el servicio vaya a interrumpirse para labores de mantenimiento, siempre fuera del referido horario, deberá comunicarse al RESPONSABLE DEL TRATAMIENTO con una antelación mínima de 48 horas.

10. SEGURO FRENTE A PÉRDIDA DE INFORMACIÓN

Con el fin de minimizar el impacto de los riesgos derivados de fallos de seguridad provocados o accidentales, que pudieran ocasionar la pérdida de información, el ENCARGADO DEL TRATAMIENTO se compromete a disponer de un seguro que cubra dichos daños, y que responda hasta un máximo de 100.000 euros.

11. PORTABILIDAD y RETORNO ORDENADO DE LA INFORMACIÓN

Una vez cumplida la prestación objeto del contrato, o bien en el supuesto de su resolución, por la causa que fuera, el ENCARGADO DEL TRATAMIENTO se obliga a entregar toda la información al RESPONSABLE DEL TRATAMIENTO en el formato que se acuerde (_____), de forma que éste pueda almacenarla en sus propios sistemas o bien optar por que se traslade a los de un nuevo proveedor en un formato que permita su utilización, en el plazo más breve posible, que no podrá ser superior a SIETE días, con total garantía de la integridad de la información y sin incurrir en costes adicionales.

El ENCARGADO DEL TRATAMIENTO se obliga a cooperar de forma activa y diligente en el marco de la migración de datos a la nueva infraestructura que, en su caso, le indique el RESPONSABLE DEL TRATAMIENTO.

NOTA: Debe pactarse un retorno ordenado de la información, estableciendo un período transitorio que permita migrar la información a otro prestador de servicios o en su caso a un CPD local. Dicho proceso deberá prever y detallar un formato de intercambio, que haga viable la extracción sin que se resienta la integridad de los datos.

12. CERTIFICADO DE ELIMINACIÓN DE DATOS

En estos casos, los datos de carácter personal que pudieran permanecer en poder del ENCARGADO DEL TRATAMIENTO –salvo que exista una norma jurídica que exija su conservación– deberán ser posteriormente destruidos, a salvo de la obligación de bloqueo de los datos impuesta por el artículo 16.3 de la LOPD, en tanto pudieran derivarse responsabilidades de su relación con el RESPONSABLE DEL TRATAMIENTO.

Pasado este plazo, el ENCARGADO DEL TRATAMIENTO debe garantizar al RESPONSABLE DEL TRATAMIENTO el borrado seguro de los datos a través de una certificación de destrucción emitido por el ENCARGADO DEL TRATAMIENTO o por una tercera entidad independiente.

13. CONTROLES Y AUDITORÍAS DEL RESPONSABLE DEL TRATAMIENTO

El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO del presente contrato. Por su parte, el ENCARGADO DEL TRATAMIENTO deberá facilitar al RESPONSABLE DEL TRATAMIENTO cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

14. SUBCONTRATACIONES Y SUBENCARGOS.

El RESPONSABLE DEL TRATAMIENTO debe autorizar previamente al ENCARGADO DEL TRATAMIENTO la intervención de entidades subencargadas que intervengan en cualquier fase del tratamiento de datos, objeto del servicio de computación en nube (reseller, agregadores de servicios de cloud, cloud builders, proveedores de aplicaciones, etc.). A tal fin, el ENCARGADO DEL TRATAMIENTO deberá realizar una solicitud formal a través de correo electrónico al RESPONSABLE DEL TRATAMIENTO, en la que se contenga informe detallado de los servicios susceptibles de subcontratación –que en ningún caso podrán ser todos los que conforman el servicio principal–, detalle de los niveles de calidad mínimos y exigibles, y declaración del subencargado candidato de sometimiento a todas las obligaciones contenidas en el presente contrato.

Una vez que el RESPONSABLE DEL TRATAMIENTO acepte la subcontratación de parte del servicio, SIEMPRE por escrito, el ENCARGADO DEL TRATAMIENTO se compromete a poner a disposición del responsable toda la información acerca de las entidades subencargadas accesible, a través de un sitio web con indicación de los países donde opera.

15. SECRETO PROFESIONAL Y CONFIDENCIALIDAD.

El ENCARGADO DEL TRATAMIENTO deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le pudieren ser entregados por el Responsable del Fichero, para la realización en cada caso de los trabajos

y servicios que pudieren acordarse, el deber de confidencialidad y secreto profesional que, de conformidad con lo dispuesto en el artículo 10 de la LOPD, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

16. EMPLEADOS DEL ENCARGADO DEL TRATAMIENTO.

EL ENCARGADO DEL TRATAMIENTO permitirá el acceso a los datos y ficheros únicamente a aquellos de sus empleados que tengan necesidad de acceder a éstos, de manera que puedan llevar a cabo sus funciones en relación con los servicios. EL ENCARGADO DEL TRATAMIENTO se obliga a no divulgar la información contenida en los ficheros en todo o en parte a personas que no tengan necesidad de acceder a ellos.

EL ENCARGADO DEL TRATAMIENTO deberá advertir a dichos empleados del carácter confidencial de la información contenida en los Ficheros y de su responsabilidad en caso de divulgarla ilícitamente. Así mismo, se compromete a comunicar y hacer cumplir a sus empleados las obligaciones establecidas en el presente contrato y, en concreto, las relativas a las medidas de seguridad.

17. EJERCICIO DE DERECHOS ARCO.

Cuando los afectados ejerciten sus derechos (de acceso, rectificación, cancelación u oposición) directamente ante el ENCARGADO DEL TRATAMIENTO y soliciten el ejercicio de su derecho ante él, el encargado debe dar traslado de la solicitud al RESPONSABLE del TRATAMIENTO en el plazo de 3 días, a fin de que por éste se resuelva.

En todo caso, el ENCARGADO DEL TRATAMIENTO debe garantizar su cooperación y las herramientas adecuadas para dar cumplida respuesta a dichos derechos.

18. PROPIEDAD INTELECTUAL.

El ENCARGADO DEL TRATAMIENTO está obligado a respetar los derechos de propiedad intelectual de los contenidos o software que el RESPONSABLE DEL TRATAMIENTO, o sus empleados, creen, almacenen o transmitan a través del software, plataforma o infraestructura.

19. TRANSFERENCIA DE CONTROL.

En el supuesto de que el ENCARGADO DEL TRATAMIENTO sea objeto de una operación mercantil de compra, absorción, fusión empresarial, u otras, la entidad resultante heredera del ENCARGADO DEL TRATAMIENTO se obliga a respetar el presente contrato, facultando, por otro lado, al RESPONSABLE DEL TRATAMIENTO a rescindirlo por esta causa, sin que dé derecho a indemnización o compensación alguna al ENCARGADO DEL TRATAMIENTO.

20. DURACIÓN DEL CONTRATO.

El presente acuerdo entrará en vigor desde la fecha de su firma y estará vigente hasta la fecha de terminación de la prestación de servicios por parte del Encargado del Tratamiento.

21. SOMETIMIENTO A ARBITRAJE EN CASO DE CONFLICTO.

Para la solución de cualquier conflicto o cuestión litigiosa derivada de este contrato, incluidos los que de ellos se deriven, así como su validez, las partes se someten al arbitraje _____ –cualquiera que fuera su denominación futura–, a quien se encomienda la designación del árbitro o árbitros y la administración del arbitraje de acuerdo con su Reglamento vigente al inicio del arbitraje.

22. NOTIFICACIONES.

Cualquier notificación que se efectúe entre las partes se hará por correo electrónico mediante el uso de firma electrónica avanzada, según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

23. CLÁUSULAS GENERALES.

La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituya una renuncia a dichos derechos en el futuro.

La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes, y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.

El presente Contrato y las relaciones entre el Responsable del Fichero y el Encargado del Tratamiento no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.

Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D./Dña. _____

En nombre de «EL RESPONSABLE DEL TRATAMIENTO»

D./Dña. _____

En nombre de «EL ENCARGADO DEL TRATAMIENTO».