Universidad Carlos III de Madrid

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

Curso académico 2019-2020

Trabajo Fin de Máster

"Informe jurídico sobre privacidad desde el diseño y seguridad de la información en una aplicación web de telemedicina"

David Salgado Arce

Tutor:

Marcos Mª. Judel Meléndrez

Madrid, julio de 2020

RESUMEN

La situación generada por la pandemia mundial de COVID-19 y los períodos de confinamiento y el distanciamiento social han traído consigo la teleactividad: el trabajo a distancia, la formación a distancia, el ocio a distancia, etc. Uno de los ámbitos en los que también se están desarrollando soluciones y herramientas a distancia es el de la medicina. La telemedicina presenta un interesante potencial desde hace años, y así son cada vez más los establecimientos y profesionales sanitarios los que comienzan a invertir en esta forma de prestar sus servicios.

Para la realización del presente trabajo se adoptará el rol de asesor jurídico al que un grupo de hospitales privados le ha solicitado un informe acerca de la elaboración de una aplicación web de telemedicina con funcionalidades que tendrán un impacto en la privacidad y la seguridad de la información que deberá abarcarse desde un enfoque práctico y desde el diseño. La inquietud del cliente es conocer las implicaciones de este tipo de herramientas y las actuaciones necesarias para cumplir la normativa aplicable.

Palabras clave: telemedicina, chatbot, privacidad, datos, eSalud.

ABSTRACT

The situation generated by the COVID-19 global pandemic and the containment periods and social distancing have led to the tele-activity: remote working, distance-learning, distance-leisure, etc. One of the areas in which distance solutions and tools are also being developed is the medicine. Telemedicine has had an interesting potential for years, and more and more health centres and professionals are beginning to invest in this mode of supply of services.

In order to carry out this work, the role of legal advisor will be adopted to whom a private hospital group has requested a report on the development of a web application for telemedicine with functionalities that will have an impact on privacy and information security, that will have to be covered from a practial and by design approach. The client´s concern is to know the implications of this kind of tools and the actions that must be carried out to comply with the applicable rules and norms.

Keywords: telehealth, chatbot, privacy, data, eHealth.

ÍNDICE DEL CONTENIDO

LISTADO DE ABREVIATURAS

AEPD: Agencia Española de Protección de Datos

CEPD: Comité Europeo de Protección de Datos

CGCOM: Consejo General de Colegios Oficiales de Médicos

CPME: Comité Permanente de Médicos Europeos

EIPD: Evaluación de Impacto en la Protección de Datos

ENS: Esquema Nacional de Seguridad

GT29: Grupo de Trabajo del Artículo 29

IA: Inteligencia Artificial

IEC: *International Electrotechnical Commission* (Comisión Electrotécnica Internacional)

ISO: *International Organization for Standardization* (Organización Internacional de Normalización)

TRLGDCU: Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios

LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

LSSI: Ley de Servicios de la Sociedad de la Información y de comercio electrónico

MIT: *Massachusetts Institute of Technology* (Instituto de Tecnología de Massachusetts)

OMS: Organización Mundial de la Salud

RGPD: Reglamento General de Protección de Datos

RLOPD: Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal

SGSI: Sistema de Gestión de la Seguridad de la Información

TFUE: Tratado de Funcionamiento de la Unión Europea

TGUE: Tribunal General de la Unión Europea

TJUE: Tribunal de Justicia de la Unión Europea

TIC: Tecnologías de la Información y la Comunicación

1. Introducción

Los sistemas sanitarios de los países desarrollados se encuentran en pleno proceso de revisión, un proceso que se ha visto fuertemente impactado por la pandemia mundial de COVID-19, que ha logrado colapsar sistemas sanitarios como los de Italia, España y Brasil[1], al menos temporalmente.

La teleactividad propiciada por los períodos de confinamiento, junto al aumento en la demanda de servicios sanitarios y factores como el envejecimiento poblacional y la cronificación han vuelto a poner el foco en las soluciones tecnológicas aplicadas al sector de la salud. Las herramientas digitales tienen el potencial de aumentar el bienestar de los ciudadanos a la par que de cambiar modelos tradicionales de prestación de servicios. De igual manera, esto es posible también en la prestación de servicios sanitarios y asistenciales, siempre que la soluciones desarrolladas en tal ámbito sean definidas, diseñadas e implantadas de forma adecuada.

Desde la Unión Europea se viene planificando un enfoque robusto de la computación de alto rendimiento, el análisis de datos y la inteligencia artificial aplicados al desarrollo de productos sanitarios innovadores, diagnósticos más rápidos y mejores y más precisos tratamientos[2].

En este sentido, el marco regulatorio europeo sigue velando por los derechos de las personas en el entorno digital, normativizando los derechos de los pacientes, la privacidad, la identificación electrónica y la seguridad de la información, entre otros, con el fin de lograr un entorno seguro, de calidad y con garantías para la libre prestación de servicios sanitarios y asistenciales digitales. Muestra de ello son el RGPD[3] y el futuro Reglamento ePrivacy[4], normas muy focalizadas en el entorno digital.

---

[1] (30 de marzo de 2020). La OMS advierte de que el colapso sanitario por el coronavirus puede aumentar las muertes de enfermedades tratables. *Infosalus*. Recuperado de: https://bit.ly/2BHCnZI.

[2] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 25 de abril de 2018, relativa a la consecución de la transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital, la capacitación de los ciudadanos y la creación de una sociedad más saludable (COM 2018/233). Recuperado de: https://bit.ly/3790SKN.

[3] 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 y por el que se deroga la Directiva 95/46/CE (DOUE núm. L 119, de 4 de mayo de 2016).

[4] Propuesta de la Comisión Europea de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (COM 2017/10).

2. Antecedentes y consideraciones previas

El presente informe ha sido encargado por H&T Hospitales, S.A., (en adelante, "H&T" o "*H&T Hospitales*", indistintamente), una importante cadena de hospitales con múltiples establecimientos en España. *H&T Hospitales* pretende desarrollar un sistema de telemedicina mediante aplicación web, con una serie de funcionalidades que serán relatadas en el apartado siguiente. Durante las conversaciones previas a la realización del presente informe, desde H&T se planteó la posibilidad de que el desarrollo y posterior mantenimiento de la aplicación fuera externalizado a una empresa especializada.

En cualquier caso, cabe destacar que la denominación de H&T responde a *Health & Tech*: se trata de una cadena de hospitales cuyo modelo de prestación de servicios sanitarios va muy unido a la tecnología y a las últimas tendencias técnicas en medicina. Su equipo de médicos especialistas de la unidad de oncología en su hospital central de Madrid, donde se encuentra igualmente el centro administrativo y de negocios de la cadena, presume de ser uno de los mejores de la Unión Europea y cuentan con dispositivos de última generación y un laboratorio volcado en el estudio de tumores de todo tipo, el diagnóstico precoz y el inmediato tratamiento.

Sin embargo, la unidad de oncología de H&T ha experimentado una merma en su actividad como consecuencia de la pandemia de COVID-19, con una bajada en la afluencia de nuevos pacientes y visitas periódicas de los ya existentes. Esto ha propiciado la decisión de implementar un sistema de telemedicina que permita a los médicos especialistas captar potenciales pacientes y atender a los ya existentes, especialmente en relación con un primer filtrado y la consulta online.

2.1. El proyecto: *H&TeHealth*

La solución tecnológica que precisa H&T se llamará *H&TeHealth*, y debe estar a la altura de la visión tecnológica de la medicina que guarda la cadena de hospitales. Evidentemente, desde H&T son conocedores de las dificultades que presenta la prestación de servicios sanitarios a distancia en relación con la oncología, pero confían en poder dar una respuesta eficaz para la pronta detección de posibles carcinomas cutáneos y melanomas; así como para atender a aquellos pacientes que puedan presentar carcinomas internos, en función de su cuadro sintomatológico, para poder derivarlos al médico especialista correspondiente en la unidad de oncología de H&T.

Partiendo de esta base, la aplicación web se dividirá en dos partes fundamentales:

1. Teleconsulta: se trata de un sistema de fijación, gestión y realización de consultas online. Los usuarios podrán adjuntar y cargar documentación en la aplicación para ser facilitada a los facultativos en el transcurso de las consultas (radiografías, informes médicos, etc.). Las teleconsultas serán objeto de contratación por parte de los usuarios, como servicio prestado por H&T a través de la aplicación.
2. Chatbot: la otra funcionalidad que interesa a H&T es la de un chatbot programado para conversar con los usuarios que lo deseen acerca de sus eventuales síntomas, de modo que mediante la recopilación de datos de los usuarios se les pueda dar una aproximación a su posible patología y recomendar ciertas acciones, así como la visita a H&T para citarse con el facultativo más adecuado en función de los resultados de la conversación. Por tanto, el chatbot enlazaría, a petición del usuario, con el sistema de consultas online de la aplicación.

Asimismo, si el usuario así lo consiente, será incluido en un sistema de envío comunicaciones comerciales por correo electrónico por parte de *H&T Hospitales*, e interesa igualmente que los datos recabados por el Chatbot puedan ser utilizados con fines estadísticos.

Las inquietudes de H&T con respecto de *H&TeHealth* engloban el impacto que esta solución tecnológica tendrá en cuanto al entorno de Internet en el que se desenvolverá, la privacidad de sus usuarios, en los datos por ella tratados, así como la seguridad de la información que se albergará y se transmitirá en aquélla.

2.2. Alcance, objetivo y metodología del informe jurídico

El empleo de técnicas de telemedicina mediante aplicaciones web, con el consecuente tratamiento de datos relativos a la salud, plantea una serie de cuestiones desde la perspectiva de la privacidad y la seguridad de la información que son las que se definirán en el presente informe, a saber:

i. Conocer las particularidades y las implicaciones jurídicas de las funcionalidades deseadas para la aplicación, desde la perspectiva de la sociedad de la información, la privacidad y la seguridad de la información.
ii. Conocer qué obligaciones y responsabilidades existen para *H&T Hospitales*, desde las perspectivas citadas.

iii. Emitir una serie de recomendaciones dirigidas a reducir o paliar riesgos relacionados con las implicaciones jurídicas de la aplicación, tras una evaluación de sus funcionalidades desde el diseño.

El presente informe jurídico, por tanto, tiene como objetivo ofrecer a H&T una serie de conocimientos, visiones y recomendaciones prácticas que les permitan conocer sus obligaciones en materia de cumplimiento normativo. El formato del documento se basará en el de un informe jurídico, por lo que la temática será abordada con cierta profundidad desde una perspectiva fáctica, normativa y jurisprudencial con vigencia en el momento de la elaboración del estudio.

Las recomendaciones repartidas a lo largo del informe serán expresadas con el siguiente formato:

Recomendación.

3. La Telemedicina como servicio sanitario

3.1. Telemedicina: concepto y tipologías

El origen de la telemedicina se remonta al origen mismo de las telecomunicaciones, con el telégrafo en el siglo XIX y la utilización masiva del teléfono en el siglo XX. Fue en abril de 1924 cuando la revista *Radio Future*[5] publicó en su portada una ilustración premonitoria en la que podía apreciarse a una persona encamada manipulando un aparato, entre radio y televisor, mediante el cual un médico le atendía a través de un micrófono y una cámara, bajo el título "*El Radio Doctor – ¡Tal vez!*".

Figura 1 - Radio News (April 1924), *THE RADIO DOCTOR - Maybe!*

Posteriormente, la telemedicina recibió diversos impulsos en las décadas de 1950 y 1970, de la mano de organizaciones como la NASA, interesada en desarrollar programas de medicina a distancia para sus astronautas[6]. El auge de Internet y los avances técnicos en las comunicaciones electrónicas han posibilitado que la telemedicina se haya asentado finalmente en el sector de la salud. La telemedicina es hoy una realidad tangible y la pandemia mundial de COVID-19 en 2020 ha acelerado la tendencia[7].

En 2008, la Comisión Europea definió los sistemas de telemedicina como aquellos que "*permiten transferir información médica a distancia por medio de tecnologías de la*

[5] *Radio News* fue una revista mensual estadounidense editada y publicada entre 1919 y 1971, inicialmente dirigida a los radioaficionados pero que terminó por ser una revista referente que recopilaba los aspectos y avances más destacables en el ámbito de la radio y la electrónica.
[6] NASA. (6 de abril de 2020). *NASA and Telemedicine*. Recuperado de: https://go.nasa.gov/2zTRL4K.
[7] López, C. Mª. (14 de abril de 2020). Los puntos cardinales de la telemedicina en tiempos de Covid-19. *Gaceta Médica*. Recuperado de: https://bit.ly/3eOHLIB.

información y la comunicación"[8]. Por su parte, la OMS define la telemedicina (*eHealth*) como la prestación de servicios sanitarios en la que pacientes y profesionales de la salud están separados en la distancia, por medio de las TIC, para el diagnóstico y tratamiento de enfermedades y lesiones, así como para investigación, evaluación y formación continua de los propios profesionales[9]. El intercambio de datos entre profesionales de la salud, y entre profesionales y pacientes, es, por tanto, la piedra angular de cualquier sistema de telemedicina.

Aunque en un principio el factor crítico de la telemedicina fue la distancia, con el fin de poder llevar la prestación de servicios sanitarios a regiones de difícil acceso en las que la distancia física entre profesional y paciente era difícilmente franqueable, la razón de ser de la telemedicina ha evolucionado a una nueva forma de prestar servicios de salud hasta convertirse en una alternativa sólida a la prestación presencial de esta clase de servicios[10].

En el campo de la oncología, las tecnologías de telemedicina resultan de especial utilidad en la asistencia en la administración de medicamentos, el asesoramiento nutricional, la orientación sobre medicamentos y tratamientos, la consultoría paliativa y sintomatológica, las revisiones médicas, etc.[11]

Dentro de la prestación de servicios de telemedicina podemos encontrar diversas tipologías en función de las características del servicio en cuestión.

Por un lado se encuentra la telemedicina de monitorización, que permite realizar un control remoto de los pacientes que sufren de, por ejemplo, enfermedades crónicas. La sensorización, la recopilación de datos y un alto ancho de banda desempeñan un papel fundamental en esta clase de telemedicina, ya que serán la fuente de información que facilite al profesional sanitario decidir sobre la necesidad o no de determinadas intervenciones[12].

---

[8] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 4 de noviembre de 2008, "La telemedicina en beneficio de los pacientes, los sistemas sanitarios y la sociedad" (COM 2008/689). Recuperado de: https://bit.ly/2A3pit3.

[9] Organización Mundial de la Salud. (13 de enero de 2011). *Global Observatory for eHealth series - Volume 2*. Recuperado de: https://bit.ly/2BrI5yA.

[10] Fundación Salud 2000. (septiembre de 2012). *Telemedicina: bases para la futura regulación de un mercado emergente* (Informe del experto Nº5). Recuperado de: https://bit.ly/2XYMPDr.

[11] American Cancer Society medical and editorial content team. (22 de abril de 2020). Telemedicina y telesalud. Recuperado de: https://bit.ly/3dK9Dh1.

[12] Lloret, J.; Parra, L.; Taha, M. y Tomás, J. (2017). An architecture and protocol for Smart continuous eHealth monitoring using 5G. *Computer Networks*, Volume 129, Part 2, pp. 340-351.

Por otro lado, encontramos la telemedicina de almacenamiento y envío, que consiste en el puro almacenamiento de datos de salud para su remisión al profesional sanitario y evaluación e interpretación por este, en tiempo real o no. Se trata de una práctica común en los campos de las especialidades médicas de la dermatología y la radiología.

Finalmente, la telemedicina interactiva permite la comunicación entre pacientes y profesionales sanitarios, y la prestación de servicios médicos, en tiempo real, a través de herramientas de videoconferencia. Esto permite servicios como la teleconsulta y el telediagnóstico. En este sentido, el CGCOM establece en el artículo 26 de su Código Deontológico[13] que la teleconsulta, como parte de la telemedicina, es éticamente aceptable para las revisiones médicas siempre que medie una "*identificación mutua y se asegure la intimidad*", así como para la orientación de pacientes y ayuda en la toma de decisiones, con la debida ampliación de las reglas de confidencialidad, seguridad y secreto. Sin embargo, cabe destacar que las consultas médicas en línea forman parte de las iniciativas europeas en materia de sanidad digital enmarcadas en la Agenda Digital para Europa[14], con acciones clave en el acceso online seguro a los datos médicos por parte de los europeos y el "*despliegue generalizado de los servicios de telemedicina*".

Por su parte, los chatbots son la unión de dos pilares fundamentales: la inteligencia artificial y la programación informática. Los chatbots obtienen resultados mediante la captación de datos, y se encuentran programados por órdenes y comandos gracias a los que el chatbot realiza acciones.

Podría decirse que su origen se remonta a 1966, cuando el profesor de informática alemán Joseph Weizenbaum, del MIT, terminó de desarrollar ELIZA, uno de los primeros programas informáticos capaces de procesar lenguaje natural y que funcionaba mediante un sistema de palabras clave[15]. Aunque la experiencia con ELIZA estuvo enfocada al ámbito psicológico de la comunicación entre persona y máquina, podríamos decir que ELIZA es la madre de los bots conversacionales modernos.

---

[13] CGCOM. (Julio de 2011). *Código de Deontología Médica: Guía de Ética Médica*. Recuperado de: https://bit.ly/2zpkoqb.

[14] Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 26 de agosto de 2010, "Una Agenda Digital para Europa", (COM 2010/245). Recuperado de: https://bit.ly/2B2trgV.

[15] Weizenbaum, J. (1976). *Computer power and human reason: from judgment to calculation*. Nueva York: W. H. Freeman and Company.

Los chatbots, hoy, son softwares regidos por una inteligencia artificial dirigida a responder automática y coherentemente a los mensajes enviados por los usuarios de aquéllos mediante el procesamiento del lenguaje natural. De esta manera, se genera una interacción en cuyo seno se mantienen conversaciones entre usuario y programa con múltiples finalidades, entre las que se pueden destacar la de facilitar información al usuario o realizar acciones determinadas relacionadas con ámbitos tales como la contratación electrónica, el marketing, la resolución de disputas y la atención al cliente[16], entre otras aplicaciones que se enmarcan en un ámbito innovador que ha pasado a denominarse comercio conversacional[17].

Incluso las instituciones han visto el potencial de los chatbots para una más eficiente y eficaz prestación de servicios públicos[18], ya que los chatbots pueden ser entrenados exponencialmente más rápido que un trabajador que deba desempeñar esta actividad, están plenamente disponibles durante las veinticuatro horas del día y, con la programación adecuada, responden y reaccionan con éxito e inmediatez a las consultas de los usuarios.

3.2. El sistema de telemedicina de *H&TeHealth*

En lo que respecta a *H&TeHealth*, la aplicación integra funcionalidades que combinan un sistema de teleconsulta, un sistema de almacenamiento y envío, y un Chatbot interactivo que permite establecer un filtrado y redireccionamiento de pacientes al profesional adecuado dentro de la unidad de oncología de H&T, en función de gravedad, estado del paciente, etc.

En lo que respecta al Chatbot, de entre las diversas tipologías de chatbot que actualmente existen en el mercado, el de *H&TeHealth* estaría por encima de los llamados chatbots de ITR[19], o "*dumb chatbots*", y se conformaría como un chatbot cognitivo, o "*smart chatbot*". El Chatbot de *H&TeHealth* es capaz de interpretar, comprender y procesar el lenguaje natural de los usuarios, formulando respuestas basadas en *Machine Learning*, es

[16] La consultora estadounidense *Gartner* estimó en un estudio de 2018 que, para este año 2020, el 25% de las operaciones de atención al cliente integrarían asistentes virtuales y tecnologías de chatbot – Moore, S. (19 de febrero de 2018). Gartner Says 25 Percent of Customer Service Operations Will Use Virtual Customer Assistants by 2020. *Gartner Press Releases*. Recuperado de: https://gtnr.it/2UjwDeW.
[17] Real, P. (25 de julio de 2018). Próxima frontera digital: el comercio conversacional. *El País*. Recuperado de: https://bit.ly/2Ui3Uay.
[18] PwC EU Services, para la Comisión Europea. (4 de septiembre de 2019). *Architecture for public service chatbots*. Recuperado de: https://bit.ly/2XY2cvW.
[19] *Interactive Text Response*, o "Respuesta de Interacción de Texto" en español. Se trata de bots conversacionales que no requieren de la aplicación de IA porque sus respuestas están predefinidas en virtud de una interacción dirigida mediante comandos.

decir, en el aprendizaje que desde H&T se le facilitará y en el generado por interacciones anteriores.

De este modo, el Chatbot podrá interactuar con nuevos usuarios no sólo para identificar el posible cuadro sintomatológico del que puedan padecer, sino también para procesar las respuestas de los usuarios y decidir a qué facultativo específico derivar al usuario en función de la información recopilada, personalizando respuestas y propuestas en este sentido. Asimismo, el Chatbot realizará un perfilado de los usuarios en función de algunos de sus datos como la edad y sus síntomas específicos con fines estadísticos.

3.3. Servicio sanitario

La Directiva de los derechos de los pacientes en la asistencia sanitaria transfronteriza[20] define en su artículo 3 la asistencia sanitaria como aquellos servicios relacionados con la salud prestados por profesionales sanitarios a pacientes para "*evaluar, mantener o restablecer su estado de salud*".

En el ámbito del ordenamiento jurídico español no existe un marco normativo expreso de la telemedicina, sin que las principales normas en materia de salud hagan referencia alguna a esta modalidad específica de prestación de servicios sanitarios. A falta de una regulación específica, a la hora de definir un sistema de telemedicina se deberán tener en cuenta, al menos, los principios básicos de la Ley General de Sanidad[21] y de la Ley de Autonomía del Paciente[22], a saber: la promoción de la salud y la prevención de enfermedades, la igualdad, la dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad, el consentimiento previo, la información adecuada al paciente, su libre decisión, etc.

En consecuencia, las funcionalidades de la aplicación, y la aplicación en sí, deberán ser definidas partiendo de estos principios y en consonancia con el resto de la normativa aplicable, que se pondrá de manifiesto posteriormente en el presente informe.

[20] Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DOUE núm. L 88, de 4 de abril de 2011).
[21] Ley 14/1986, de 25 de abril, General de Sanidad (BOE núm. 102, de 29 de abril de 1986).
[22] 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 (BOE núm. 274, de 15 de noviembre de 2002).

Desde H&T se ha planteado la duda sobre si una solución tecnológica como *H&TeHealth* podría considerarse como un producto sanitario, ya que el artículo 1.2 de la Directiva relativa a los productos sanitarios[23] define los mismos como "*cualquier instrumento, dispositivo, equipo, programa informático, material u otro artículo*" destinado a ser utilizado con fines de diagnóstico, prevención, control, tratamiento o alivio de una enfermedad o lesión. El TJUE ha despejado esta duda, ya que ha declarado, en el ámbito de la asistencia sanitaria y la comercialización de programas informáticos de ayuda a la prescripción médica mediante la explotación de datos, que los softwares para usos generales utilizados en el marco de la asistencia sanitaria "*no son productos sanitarios*"[24]. En el caso, un programa informático diseñado para cotejar datos de pacientes y medicamentos prescritos por el correspondiente facultativo para proporcionar un análisis sobre contraindicaciones, interacciones y posologías excesivas, con fines de prevención, control, tratamiento o alivio de enfermedades, encajaba en el ámbito de aplicación del concepto de producto sanitario.

Si bien es cierto que el sistema de telemedicina de *H&TeHealth* integra funcionalidades como un sistema de consultas online y un chatbot, estas no dejarían de ser funcionalidades generales en el marco de la teleasistencia prestada por los profesionales de la unidad de oncología de *H&T Hospitales*. La aplicación, aun utilizada en un entorno sanitario, simplemente archivaría, recopilaría y transmitiría datos. En este sentido, la Comisión Europea ha indicado que los programas informáticos cuya acción se limita al almacenamiento, comunicación y compresión de datos, como bibliotecas digitales, no son productos sanitarios regidos por la Directiva[25]. Seguimos hablando, por tanto, de un servicio sanitario.

Volviendo a los principios sobre los que el sistema de telemedicina deberá articularse, encontramos que tanto la doctrina[26] como el CPME, en sus primeras directrices éticas sobre la telemedicina[27], resaltan algunas características importantes.

---

[23] Directiva 93/42/CEE del Consejo, de 14 de junio de 1993, relativa a los productos sanitarios (DOCE núm. L 169, de 12 de julio de 1993).
[24] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Cuarta), de 7 de diciembre de 2017 (asunto C-329/16). Disponible en: https://bit.ly/2Yl89mX.
[25] Comisión Europea. (Julio de 2016). *Guidelines on the qualification and clasiffication of stand alone software used in healthcare within the regulatory framework of medical devices* (MEDDEV 2.1/6). Recuperado de: https://bit.ly/2AipMvB.
[26] Mercado Carmona, C. (2005). La eSalud y el Derecho. *Revista eSalud*, Vol. 1 (nº2), p. 3.
[27] CPME. (abril de 1997). *Ethical Guidelines in telemedicine* (CP 97/033). Recuperado de: https://bit.ly/3hiXfa4.

Por ejemplo, los cambios en la relación médico-paciente en relación con la prestación a distancia, donde la obligación de identificación por parte del facultativo no decae, así como la obligación de obtener un historial completo del paciente con el fin de que todos los casos sigan estando debidamente documentados. De ahí, por tanto, el carácter trascendental de que, aun tratándose de una prestación a distancia, el equipo de H&T pueda obtener documentos facilitados por los usuarios de *H&TeHealth* y, así, documentar cada caso y seguir formando la historia clínica del paciente.

Con el fin de asegurar la identidad de las partes y una garantista transmisión de información entre ambas, se recomienda que el acceso al sistema de *H&TeHealth* se realice mediante alguna clase de certificado electrónico para limitar suplantaciones de identidad. Por ejemplo, podría articularse, adicionalmente al sistema de usuarios y claves, un sistema de acceso paralelo mediante documento nacional de identidad electrónico o tarjeta sanitaria electrónica.

Los facultativos de H&T, por su parte, deberán facilitar sus datos profesionales, de contacto y del cargo y centro al que pertenecen, para no dejar lugar a dudas en el usuario paciente de que el profesional al que se dirige a través de una teleconsulta tiene la cualidades que se le presuponen para la prestación del servicio.

Además de lo establecido por la Directiva 2011/24/UE con respecto de la telemedicina como servicio sanitario, no se debe obviar el hecho de que la telemedicina, como servicio de asistencia sanitaria, se encuentra regulada en los artículos 56 y 57 del TFUE[28], en relación con la libre prestación de servicios en la Unión Europea y la consideración como servicio de "*las prestaciones realizadas normalmente a cambio de una remuneración*".

Partiendo de esta base, el servicio de telemedicina deberá ser prestado cumpliendo con la regulación europea y española aplicable en materia de Internet, protección de datos y seguridad de la información.

3.3.1. El consentimiento informado

El consentimiento informado se conforma como otro de los pilares fundamentales con los que deberá contar el sistema de telemedicina de H&T, tal y como recoge la Ley de

[28] Versión consolidada del Tratado de Funcionamiento de la Unión Europea (DOUE núm. C 83, de 30 de marzo de 2010).

Autonomía del Paciente en sus artículos 2, 4 y 8. Es una cuestión básica en la relación entre pacientes y médicos, y por regla general será verbal. No obstante, deberá figurar por escrito cuando el tratamiento o prueba a realizar entrañe un riesgo notorio para la salud del paciente: intervenciones quirúrgicas, procedimientos terapéuticos y diagnósticos invasores, etc.

En el caso de las teleconsultas de *H&TeHealth*, el consentimiento informado podrá prestarse verbalmente, ya que no existe riesgo notorio alguno en el tratamiento del usuario paciente.

Se recomienda articular un mecanismo a través del cual se pueda informar a los usuarios sobre la finalidad, la naturaleza y las consecuencias del servicio de teleconsultas prestado a través de *H&TeHealth*, ya que ello puede tener un impacto importante en ulteriores depuraciones de responsabilidades ante un eventual daño sufrido por el paciente[29].

Por ejemplo, podría implantarse un paso previo a la contratación de una teleconsulta en el que se facilitara esta información al usuario, que deberá manifestar haber leído antes de proceder al proceso de contratación de una consulta online en el correspondiente formulario de la aplicación.

Otra opción sería incluir esta información en las Condiciones Generales de Contratación del servicio de teleconsultas de la aplicación (**Anexo II**), siempre que exista la certeza de que el usuario ha leído y comprendido la información.

La opción más garantista pasa por facilitar la información al usuario de forma separada de las Condiciones Generales de Contratación, en formato descargable, en una ventana automática y previa al proceso de contratación de teleconsultas, con un enlace al formulario de contacto de la aplicación para aquellos casos en que el usuario tenga alguna duda con respecto de la información facilitada antes de proceder a prestar su consentimiento a ser sujeto del servicio de teleconsulta de *H&TeHealth*.

[29] Martínez Zaporta, E. (2008). Telemedicina y responsabilidad patrimonial de la Administración Sanitaria. *Revista Española de Administración Sanitaria*, Vol. 16 (nº1), pp. 109-134.

4. Sociedad de la Información

4.1. Calificación como servicio de la sociedad de la información y como prestador de servicios de la sociedad de la información

Los portales y las plataformas, sitios de Internet en los que se ofertan servicios e información dotada de un orden y una estructura determinadas, han pasado a ocupar un lugar de absoluta centralidad en el suministro de contenidos y servicios en la sociedad de la información. Entre estas prestaciones podemos encontrar servicios tales como el acceso a Internet, el correo electrónico, el hospedaje de páginas web, etc. Sin embargo, como señala BARRIO ANDRÉS, la lista de servicios de la sociedad de la información debe considerarse como *numerus apertus*[30], ya que con el paso del tiempo surgen nuevas necesidades y los proveedores de servicios van ampliando sus catálogos de prestaciones, incluso con aplicaciones a medida como es *H&TeHealth*, la aplicación objeto del presente informe.

La definición jurídica de lo que debemos entender por servicio de la sociedad de la información fue establecida por la ya derogada Directiva 98/34/CE[31], como "*todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios*". Estas son las notas que se deben abordar a la hora de dictaminar acerca de la naturaleza de *H&TeHealth* como servicio de la sociedad de la información.

Esta definición ha sido igualmente recogida, primero, en las Directivas sobre el comercio electrónico[32] y los servicios de la sociedad de la información[33], y posteriormente en la transposición de dichas Directivas en el ordenamiento jurídico español, con la LSSI[34].

[30] Barrio Andrés, M. (2017). *Fundamentos del Derecho de Internet*. Madrid: Centro de Estudios Políticos y Constitucionales.
[31] Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas (DOCE núm. L 204, de 21 de julio de 1998).
[32] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DOCE núm. L 178, de 17 de julio de 2000).
[33] Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DOUE núm. L 241, de 17 de septiembre de 2015).
[34] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166, de 12 de julio de 2002).

Así, encontramos por un lado la nota "*a cambio de una remuneración*", refiriéndonos en este caso a una actividad económica que busca una rentabilidad que puede estar sustentada con ingresos directos por parte del usuario o indirectos como los derivados de las actividades de publicidad y patrocinio. El TJUE ha establecido que la retribución reside en la prestación que la motiva[35], pero en el caso de los servicios de la sociedad de la información adquiere especial relevancia el solo hecho de la concurrencia de una actividad económica, como hemos indicado, ya que los servicios a título gratuito también encuentran cabida en el concepto de servicio prestado a cambio de una remuneración toda vez que este sea parte de una actividad económica. Además, como indica LÓPEZ-MONÍS, lo importante es que "*en condiciones normales del tráfico se exija por el prestador una contraprestación, con independencia de que en cada caso concreto se haya satisfecho o no la oportuna contraprestación*"[36].

Por otro lado, servicios prestados "*a distancia*", que supone que las partes no estén simultáneamente presentes en la prestación del servicio sanitario a través de *H&TeHealth*. Asimismo, la nota de la "*vía electrónica*" hace referencia a los servicios prestados mediante equipos electrónicos de tratamiento y almacenamiento de datos que se transmiten por medios igualmente electrónicos, definición en la que vuelve a encajar el sistema de telemedicina de H&T.

Finalmente, la nota relativa a la "*petición individual de un destinatario de servicios*" se refiere a la transmisión de datos punto a punto entre, en este caso, usuario/paciente y facultativo de H&T, actuando este último en el ámbito de su actividad profesional.

En definitiva, el sistema de telemedicina de *H&TeHealth* ha de ser considerado no sólo como servicio sanitario sino, además, como servicio de la sociedad de la información, naturaleza a la que se asocian una serie de obligaciones y responsabilidades que se recogen a continuación.

Asimismo, en relación con *H&T Hospitales*, como titular de la aplicación a través de la que se prestará el servicio de telemedicina, el control de origen de la normativa comunitaria y de la LSSI establece que esta última será aplicable a aquellos prestadores

[35] Sentencia del Tribunal de Justicia de la Unión Europea de 11 de abril de 2000 (asuntos acumulados C-51/96 y C-191/97). Disponible en: https://bit.ly/30pjGnO.
[36] López-Monís, M. (2003). Ámbito de aplicación de la nueva Ley de Servicios de la Sociedad de la Información y de comercio electrónico. En *Derecho de Internet: la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico* (pp. 25-64). Madrid: Aranzadi.

de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos, entendidos aquéllos como prestadores con residencia o domicilio social en territorio español, así como el lugar de centralización de la gestión administrativa y la dirección de los negocios del prestador. Tal es el caso de la cadena de hospitales de H&T, que centraliza su administración en su sede de Madrid, donde se encuentra la unidad de oncología especializada que encarga la aplicación objeto del presente informe.

Debemos concluir, por tanto, que H&T, como prestador de servicios sanitarios que cumple asimismo con el ámbito de alcance del concepto de servicio de la sociedad de la información y prestador de este con la aplicación *H&TeHealth*, deba complementar su adhesión a la normativa sectorial sobre salud anteriormente citada con la relativa a la sociedad de la información.

4.2. Obligaciones y responsabilidades

Los servicios de la sociedad de la información se rigen por el principio de libre prestación y la no autorización previa. No obstante, esto no es obstáculo para que se impongan a los prestadores algunas obligaciones adicionales con el fin de lograr lo que el espíritu de la normativa pretende: la seguridad jurídica y la confianza de los destinatarios de servicios de la sociedad de la información[37].

Por ejemplo, la no autorización previa no es motivo para no exigir la autorización debida, en el ámbito sanitario, al facultativo de H&T que se identifique como tal ante los usuarios de *H&TeHealth*, ya que ello respondería al régimen de autorización de la actividad específica de la medicina (la posesión de un título expedido por la autoridad competente, planes de especialidad, etc.).

4.2.1. Información general

La LSSI recoge como obligación expresa de todos los servicios de la sociedad de la información la de información general, en su artículo 10. Esta obligación responde a la necesidad de que los consumidores y usuarios, destinatarios del servicio, puedan identificar y localizar al prestador que se encuentra tras el servicio en cuestión.

[37] Márquez Lobillo, P. (2007). Obligaciones y responsabilidades de los empresarios y los profesionales en la sociedad de la información. En *Empresarios y profesionales en la sociedad de la información* (pp. 287-407). Madrid: Edersa.

De esta manera, se deben articular mecanismos mediante los cuales los destinatarios puedan acceder a la información debida electrónica, permanente, fácil, directa y gratuitamente.

Se recomienda la elaboración y disposición en la aplicación de un **Aviso Legal** (disponible en el **Anexo I** del presente informe) que contemple la siguiente información:

i. Identificación del prestador: denominación social de H&T, su domicilio, número de identificación fiscal, una dirección de correo electrónico de contacto, y los datos registrales de la organización.
ii. Información específica sobre la actividad: habida cuenta de la naturaleza de servicio sanitario que entraña *H&TeHealth*, con el objetivo de lograr una mayor transparencia y, ante todo, un mayor grado de confianza de los destinatarios, se recomienda incluir los datos de colegiación de los facultativos de la unidad de oncología de H&T que atenderán telemáticamente a los usuarios.

Se recomienda igualmente la elaboración y disposición en la aplicación de un apartado de **Condiciones de Uso** (disponibles en el **Anexo I**) que recojan las notas reguladoras del acceso, registro y uso de la aplicación web *H&TeHealth*, así como cualquier otra cuestión como las relativas a las condiciones que regulen la eventual reserva de espacios publicitarios a través de la aplicación, en su caso.

4.2.2. Contratación electrónica

En relación con la contratación electrónica del servicio de teleconsulta prestado por H&T a través de *H&TeHealth*, el artículo 23 de la LSSI establece los requisitos para la validez y eficacia de los contratos celebrados por vía electrónica, entre los que se destaca el consentimiento además del resto de los requisitos generales de la contratación civil y mercantil (causa y objeto). Será de aplicación paralela, igualmente, la legislación de defensa de consumidores y usuarios, ya que los destinatarios de los servicios prestados serán personas físicas que acudan a *H&TeHealth* con un propósito ajeno a su actividad profesional o empresarial, concepto que también comparte la jurisprudencia europea[38]. Esta legislación recoge una serie de requisitos de los contratos a distancia, entre los que

[38] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Cuarta), de 3 de septiembre de 2015 (asunto C-110/14). Disponible en: https://bit.ly/2UChNR9.

destacamos la información precontractual sobre las características de, en este caso, los servicios sanitarios a distancia ofertados en *H&TeHealth*.

Se recomienda la elaboración y disposición en la aplicación de un apartado de **Condiciones Generales de Contratación** (disponibles en el **Anexo II** del presente informe) que recoja los términos reguladores de la contratación del servicio de teleconsulta de la aplicación: aspectos como los medios de pago admitidos, la lengua de formalización del contrato, requisitos, garantías contractuales y las condiciones de desistimiento, entre otros.

Sobre el desistimiento, el artículo 103.a) del TRLGDCU[39] establece que este derecho no se aplicará cuando el servicio haya sido completamente ejecutado, con consentimiento expreso del consumidor y usuario.

Se recomienda poner este hecho en conocimiento de los usuarios de la aplicación mediante un apartado específico en las Condiciones Generales de Contratación.

4.2.3. Cookies

Las Cookies están recogidas en el artículo 22.2 de la LSSI, como dispositivos de almacenamiento y recuperación de datos. En caso de que la aplicación las utilice, se deberá informar a los usuarios de tal extremo en la forma marcada por las más recientes directrices de la AEPD al respecto[40].

Se recomienda la elaboración y disposición en la aplicación de una **Política de Cookies** (disponible en el **Anexo III** del presente informe) en la que se informe a los usuarios sobre la descarga y uso de estos dispositivos, las tipologías de Cookies utilizadas, las finalidades de su utilización, la información recopilada por ellas, etc.

Asimismo, se deberá disponer de una primera capa informativa en la que se facilite información básica sobre las Cookies eventualmente utilizadas en *H&TeHealth*. A menudo, esta primera capa se muestra en forma de *banners* o *pop-ups* en el momento de iniciarse la sesión de navegación, en un paso previo sin descarga de Cookies hasta que el

[39] Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (BOE núm. 287, de 30 de noviembre de 2007).
[40] AEPD. (2019). *Guía sobre el uso de las cookies*. Recuperado de: https://bit.ly/3dYREDJ.

usuario preste su consentimiento expreso a la utilización y descarga de estos dispositivos[41]. Se facilita texto del aviso de primera capa en el **Anexo III**.

De esta manera, la Política de Cookies incluirá información más completa y extensa sobre la utilización de cookies en *H&TeHealth*, en la llamada segunda capa de información.

Se recomienda que el aviso de primera capa cuente con un botón que permita la oposición a la descarga de cookies desde el comienzo de la sesión, así como la fijación de un panel de configuración que permita al usuario configurar las cookies en función de su procedencia, tipologías y finalidades.

Aunque no existe norma alguna acerca de la forma en que deben presentarse todos los textos legales citados en este apartado, desde esta Firma se recomienda siempre disponerlos individualmente en forma de enlaces a los textos en el *footer* o pie de página de la aplicación web, garantizando la transparencia y una mayor claridad de cara a los usuarios, que podrán encontrar toda la información relevante sobre *H&TeHealth* en una suerte de directorio de enlaces de fácil acceso. Asimismo, los textos legales deberán ser legibles, por lo que se recomienda un tamaño de letra lo suficientemente grande y con suficiente contraste entre color de letra y el del fondo de la página.

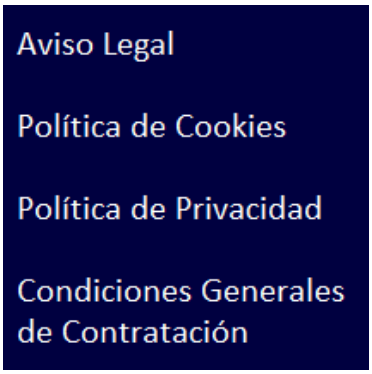

Figura 2 - Ejemplo de disposición de enlaces a textos legales en la aplicación.

Finalmente, cabe destacar que la LSSI contempla en su Disposición Adicional Novena una obligación general de colaboración en la resolución de incidentes de ciberseguridad

[41] Cabe hacer hincapié en este punto, ya que la AEPD es especialmente prolija en su actividad sancionadora contra prestadores de servicios de la sociedad de la información por infracción del artículo 22 de la LSSI. Las causas de sanción más comunes son las faltas de transparencia en la información sobre Cookies y la no obtención del consentimiento del usuario. Algunos de los casos más recientes han sido una multa a IKEA de 10.000 euros (Procedimiento PS/00127/2019: https://bit.ly/2YxwZzR) y una de 30.000 euros a Twitter (Procedimiento PS/00299/2019: https://bit.ly/2zwCt5I).

con el Equipo de Respuesta ante Emergencias Informáticas correspondiente, que en el caso de ciudadanos y empresas es la entidad INCIBE-CERT[42]. La naturaleza de los datos que se estarán tratando en *H&TeHealth*, relativos a la salud, hacen a la aplicación especialmente vulnerable en caso de brecha o violación de seguridad. En el siguiente apartado y en el apartado 6 del presente informe, sobre seguridad de la información, se abordarán una serie de recomendaciones para paliar riesgos en este sentido.

[42] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 218, de 8 de septiembre de 2018).

5. Protección de datos

H&TeHealth, a través de sus funcionalidades de teleconsulta y Chatbot, vendrá a recopilar datos, procesarlos y responder a sus finalidades con base en ellos, mediante los usuarios que interactúen con la aplicación.

En este sentido, todo tratamiento de datos de carácter personal llevado a cabo en la aplicación deberá sustentarse en la información a los usuarios, una base de legitimación adecuada y la garantía de los principios del tratamiento de datos recogidos en el artículo 5 del RGPD: licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad; y, por último, la responsabilidad proactiva del titular de *H&TeHealth*, es decir, el Responsable del tratamiento de los datos tratados por esta[43], *H&T Hospitales*.

Asimismo, la privacidad desde el diseño y por defecto desempeñarán un papel fundamental en la configuración de la aplicación.

5.1. Datos relativos a la salud

Como se ha indicado anteriormente, la telemedicina se basa fundamentalmente en los flujos de datos entre profesionales y entre pacientes y profesionales de la salud. El impacto en la privacidad de los usuarios de un servicio de telemedicina online es evidente, y la garantía de un ecosistema de telemedicina que vele por la privacidad del usuario/paciente y la seguridad del sistema son cuestiones fundamentales de las que depende directamente la confianza en esta modalidad de prestación de servicios sanitarios[44], con la intervención de las autoridades de control y el marco regulatorio común facilitado por el RGPD.

Como rezan los artículos 2 y 3 del RGPD, este será aplicable al tratamiento total o parcialmente automatizado de datos personales en el contexto de un establecimiento del responsable o del encargado en la Unión, de interesados residentes en la Unión cuando el tratamiento se relacione con la oferta de bienes o servicios a tales interesados. Tal es el

[43] Sánchez, L. J. (20 de octubre de 2018). Configurar un chatbot supone ya aplicar para la empresa creadora los nuevos principios de privacidad que exige el RGPD. *Confilegal*. Recuperado de: https://bit.ly/2UHU0z6.

[44] Edmunds, M.; Tuckson, R.; Lewis, J. y Atchinson, B. (2017). An Emergent Research and Policy Framework for Telehealth. *eGEMs (Generating Evidence & Methods to improve patient outcomes)*, Vol. 5. Recuperado de: https://bit.ly/3f4N1rW.

caso de H&T, que estará ofertando servicios sanitarios a distancia, telemedicina, en su establecimiento de Madrid, a interesados residentes en España y en la Unión Europea.

En cuanto al concepto de datos personales, el antiguo GT29, hoy transformado en el CEPD, estableció los cuatro componentes fundamentales de los que consta la definición de datos personales[45]: "*toda información sobre una persona física identificada o identificable*". En primer lugar, el sentido amplio que otorga al concepto de dato personal la nota "*toda información*" (es decir, toda clase de afirmaciones sobre una persona que proporcionen información sobre esta). En segundo lugar, la relación establecida por la nota "*sobre*" (información referida a una persona física). En tercer lugar, el hecho o la posibilidad de identificar que añade la nota "*[persona física] identificada o identificable*" (mediante identificadores relacionados con una persona en la información). En cuarto y último lugar, la nota "*persona física*", el eje y objeto de la protección de los datos personales. Debemos entender, por tanto, que mediante *H&TeHealth* se estarán tratando diversas tipologías de datos de carácter personal, tales como datos identificativos y de contacto (nombres, apellidos, documentos de identidad, direcciones de correo electrónico, números de teléfono, etc.), datos sobre características personales (sexo, edad, estatura, peso, actividades deportivas, etc.), datos laborales y datos especialmente protegidos.

En este sentido, precisamente, la telemedicina tiene un impacto en la privacidad más hondo, si cabe, habida cuenta de que dentro de los flujos de datos citados encontraremos datos relativos a la salud, es decir, una de las categorías especiales de datos personales del artículo 9 del RGPD. El tratamiento de tales datos sería posible por el consentimiento explícito del interesado, pero, sin embargo, en la prestación de servicios sanitarios, como se indicará más adelante, el tratamiento de datos relativos a la salud será realizado por los profesionales y centros sanitarios con base en la ejecución de un contrato en el que el interesado es parte, para la prestación de tales servicios (véase **apartado 5.4.2.3**).

La jurisprudencia europea ha dictaminado[46] que debe darse una interpretación amplia a la expresión "*datos relativos a la salud*" que figura en el derogado Reglamento 45/2001[47],

[45] GT29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales* (WP 136). Recuperado de: https://bit.ly/37sBpwj.
[46] Sentencia del Tribunal General de la Unión Europea (Sala Sexta), de 3 de diciembre de 2015 (asunto T-343/13). Disponible en: https://bit.ly/2zek4dC.
[47] Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las

hoy Reglamento 2018/1725[48], de forma que estos datos comprendan toda la información relacionada con todos los aspectos, físicos y psíquicos, de la salud de las personas. Precisamente el artículo 3 del Reglamento 2018/1725 define los datos relativos a la salud como aquellos "*relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud*", tal y como también hace el artículo 4 del RGPD. Por su parte, tanto el Considerando 37 del Reglamento 2018/1725 como el Considerando 63 del RGPD hacen especial hincapié en el derecho de los interesados a acceder a los datos de salud de sus historias clínicas que contengan diagnósticos, resultados, evaluaciones, intervenciones, etc., con el fin de obtener la información sobre el tratamiento de tales datos: los fines del tratamiento, el plazo de este, los destinatarios, la lógica tras el tratamiento automático, elaboración de perfiles, etc.

De esta manera, en la elaboración de un sistema de telemedicina se deberá articular previamente, y con una centralidad absoluta, la forma en que los usuarios del sistema podrán ejercer sus derechos de protección de datos en lo que respecta a los datos de salud tratados en aquél; más, si cabe, cuando nos encontramos ante un tratamiento que, a grandes rasgos, se realizará en un entorno digital y online.

En lo que respecta a *H&TeHealth*, se estarán recopilando y tratando datos de carácter personal de los usuarios, entre los que se encontrarán datos relativos a la salud tanto en el caso del Chatbot de la aplicación como en el caso de las teleconsultas. En un caso y otro, el usuario de *H&TeHealth* podrá facilitar datos mediante el uso del lenguaje natural o mediante su transmisión a través de la aplicación, en forma de documentos, imágenes y demás soportes de datos.

5.2. Sujetos implicados

En el desenvolvimiento de la aplicación *H&TeHealth* concurren, a grandes rasgos, las siguientes partes implicadas:

instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOCE núm. L 8, de 12 de enero de 2000).

[48] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE (DOUE núm. L 295, de 21 de noviembre de 2018).

i. **H&T Hospitales, S.A.,** como titular de la aplicación y persona jurídica que estará determinando los fines y medios del tratamiento de datos a través de aquélla, H&T se conforma como Responsable del tratamiento, desempeñando un papel primordial en el cumplimiento de las normas de privacidad y seguridad de la información[49].

ii. **Usuarios,** como todos aquellos usuarios pacientes, interesados, que utilicen la aplicación, facilitando sus datos a través de formularios y/o en la interacción con el Chatbot de *H&TeHealth*.

iii. **Encargados del tratamiento**, como aquellas personas físicas o jurídicas que estarán tratando datos de responsabilidad de H&T, a cuenta de esta y bajo sus instrucciones, en el marco de, por ejemplo, la prestación de servicios determinados (servicios cloud, mantenimiento de redes y/o software, etc.).

5.3. Análisis de riesgos inicial

Basta acceder a la herramienta para tratamientos de escaso riesgo facilitada por la AEPD, *Facilita*[50], para concluir que el tratamiento de datos llevado a cabo a través de la aplicación requerirá de un análisis de riesgos, toda vez que existen datos relativos a la salud involucrados y que el titular de aquélla, *H&T Hospitales*, es una organización del sector de la Sanidad.

Con el fin de gestionar los riesgos concernientes al tratamiento de datos en *H&TeHealth*, es preciso comenzar realizando un breve análisis inicial a través del cual se puedan identificar amenazas, evaluar riesgos y tratarlos de forma adecuada. A priori, categorizaremos las amenazas en virtud de tres clases generales presentes en cualquier tratamiento de datos: acceso ilegítimo a los datos, modificación no autorizada de estos y su eliminación. El daño eventualmente causado por la materialización de alguna de estas amenazas se desenvolvería, respectivamente, en los ámbitos de la confidencialidad la integridad y la disponibilidad de los datos.

[49] GT29. (2010). *Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"* (WP 169). Recuperado de: https://bit.ly/2YxDIdk.

[50] Al acceder a la herramienta a través de la URL https://bit.ly/380Y5Up, se muestra un listado inicial de sectores de actividad entre los que encontramos la Sanidad, la Solvencia patrimonial y crédito, los Seguros, etc. Si la actividad de la organización pertenece a alguno de ellos, la herramienta nos comunica automáticamente que se debe realizar un análisis de riesgos.

Como señala la AEPD[51], la definición de las actividades de tratamiento deviene fundamental, con una correcta identificación de sus finalidades, bases jurídicas y grupos de interesados afectados por el tratamiento, en virtud del citado artículo 5 del RGPD.

De este modo, en el caso de *H&TeHealth* concurren una serie de criterios tales como la evaluación en términos de salud, el tratamiento de datos altamente confidenciales como aquellos relativos a la salud de los usuarios pacientes de la aplicación, el uso de aplicaciones y soluciones tecnológicas como la que es objeto del presente informe, y la sujeción a códigos de conducta como pueden ser, por ejemplo, las normas éticas de la medicina citadas con anterioridad. Todos estos criterios, junto al tratamiento a gran escala de miles de usuarios, hacen que el tratamiento de datos llevado a cabo en la aplicación entrañe un **alto riesgo** para los derechos y libertades de los interesados.

En cuanto al Chatbot y el uso de IA por parte de H&T, el tratamiento de datos contribuye al entrenamiento de sistemas de *machine learning* y, así, construir sus modelos algorítmicos. Es posible que las predicciones y decisiones hechas por un sistema de IA sean más precisas e imparciales que las de un humano, ya que el objeto es que la inteligencia artificial evite las falacias típicas de la psicología humana y se sujete a controles rigurosos. Sin embargo, existe un riesgo de que las decisiones algorítmicas estén equivocadas o sean discriminatorias[52]. En el ámbito del sistema de salud, y en la medicina en general, la accesibilidad a los servicios sanitarios en condiciones de igualdad se conforma como uno de los principios generales. De este modo, los bots deberán actuar e interaccionar de la misma manera con todos los usuarios. El riesgo reside en que quien programa un Chatbot puede estar programando en él, a veces de forma incluso

[51] AEPD. (2018). *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*. Recuperado de: https://bit.ly/3dzUkXa.

[52] Existe un precedente reciente sobre casos en que diversas IA han desarrollado respuestas discriminatorias. En Estados Unidos existe un software, *Compas*, que sirve para predecir si personas arrestadas y condenadas podrían reincidir, generando una serie de "puntuaciones de riesgo" que en algunos Estados como Virginia y Oklahoma forman parte del proceso de juzgamiento. Sin embargo, un estudio constató que el algoritmo de *Compas* tendía a asignar puntuaciones de riesgo más altas a personas de raza negra, justificándose aparentemente en circunstancias socioeconómicas – Letzter, R. (23 de mayo de 2016). This software that helps predict criminal behavior is under fire for having a "racist" algorithm. *Business Insider*. Recuperado de: https://bit.ly/2zI3jYI. Asimismo, *Tay*, una IA diseñada por *Microsoft* para procesar lenguaje natural y conversar con personas de entre 18 y 24 años a través de *Twitter* para, así, aprender, terminó emitiendo mensajes sexistas y xenófobos tras apenas 24 horas de funcionamiento – (28 de marzo de 2016). Una inteligencia artificial se vuelve racista, antisemita y homófoba en menos de un día en Twitter. *El Mundo*. Recuperado de: https://bit.ly/37BQICO.

inconsciente, una serie de prejuicios que, a la postre, generarán discriminaciones en el tratamiento y procesamiento de datos que llevará a cabo el bot conversacional[53].

El riesgo a que este tipo de amenazas, propias de la utilización de IA, se materialice aumentará proporcionalmente al tipo de IA que se utilice en cada momento, ya que un "dumb bot" no presenta el mismo nivel de riesgo de producir situaciones discriminatorias que un "smart bot", que procesa el lenguaje natural, aprende de él y confecciona nuevas respuestas no necesariamente programadas previamente. Por tanto, el objetivo de aunar RGPD e IA es la adecuada delimitación de las finalidades de un sistema como el bot conversacional de *H&TeHealth* y el respeto del principio de minimización de los datos desde una perspectiva de reducción de la personalidad de los datos[54].

En relación con la aplicación en sí, existen amenazas para la confidencialidad de los datos tratados en *H&TeHealth* en tanto en cuanto no se articule debidamente la relación existente entre el Responsable y el eventual Encargado que vaya a dedicarse a desarrollar y mantener la aplicación, que podría tener acceso a los datos si no resulta ser el Encargado adecuado, como se ha indicado previamente en este informe (véase **apartado 5.6**).

Finalmente, existen amenazas más habituales asociadas a la propia naturaleza de las aplicaciones web, como el acceso ilegítimo a los datos por parte de terceros, tanto intencionada como accidentalmente; la eliminación de datos como consecuencia de ataques o casos de fuerza mayor, etc., que tendrán un impacto en la confidencialidad, la integridad y la disponibilidad de la información. El riesgo en estos casos, ante un sistema de información adecuadamente protegido y protocolizado, puede verse reducido a un mínimo asumible, como se pondrá de manifiesto al tratar la seguridad de la información en *H&TeHealth* en el apartado 6 del presente informe.

La forma de minimizar los riesgos detectados en los tratamientos de *H&TeHealth* será la aplicación de una privacidad desde el diseño y por defecto en la aplicación.

[53] Laukyte, M. (2018). Robots y Sanidad. En *Sociedad Digital y Derecho* (p. 865-878). Madrid: Publicaciones Oficiales BOE.
[54] Panel for the Future of Science and Technology of the European Parliament. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (PE 641.530). Recuperado de: https://bit.ly/2YyLCnZ.

5.4. Privacidad desde el diseño y por defecto

El artículo 25 del RGPD establece una obligación general para los Responsables del tratamiento consistente en aplicar medidas técnicas y organizativas apropiadas "*para aplicar de forma efectiva los principios de protección de datos*", integrando garantías en el tratamiento y protegiendo los derechos de los interesados. Asimismo, se establece la obligación de que el Responsable aplique igualmente medidas para garantizar que, por defecto, "*sólo sean objeto de tratamiento los datos personales que sean necesarios pata cada uno de los fines específicos del tratamiento*". Esto es lo que conoce como la privacidad desde el diseño y por defecto.

Como indica CAVOUKIAN[55], la privacidad desde el diseño descansa sobre la proactividad, una adecuada configuración de privacidad por defecto, la protección integral en el ciclo de vida de los datos, la visibilidad y la transparencia, y la centralidad del usuario, en un sistema centrado en este. En este sentido, todos los sujetos implicados en el tratamiento de datos deben aplicar enfoques desde el diseño en aquél. Por ejemplo, se alienta a los desarrolladores de software para que observen el derecho a la protección de datos a la hora de diseñar productos y servicios tales como es, en este caso, la aplicación objeto del presente informe[56], incluso en su papel ocasional de Encargados del tratamiento, del que se hablará posteriormente.

Sin perjuicio del marco normativo del RGPD, en aplicación desde mayo de 2018, con la posterior llegada de la LOPDGDD en diciembre del mismo año, es preciso resaltar lo que la Disposición Adicional Única del RLOPD[57] dispone en relación con los productos de software, ya que sigue con numerosos aspectos en vigor, y es que los productos de software que vendrán a tratar datos personales automáticamente deberán incluir una descripción técnica sobre el nivel de seguridad del producto. La AEPD, por su parte, ha incidido igualmente en la necesidad de que esta clase de productos incorporen

[55] Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Recuperado de: https://bit.ly/3e2AepB.

[56] Recientemente, la autoridad nacional de control francesa, la CNIL, ha publicado una guía de cumplimiento del RGPD especialmente dirigida a los desarrolladores tecnológicos, que contempla diversas fases a tener en cuenta desde una perspectiva de privacidad desde el diseño y por defecto: identificación de datos, preparación del desarrollo, aseguramiento del entorno de desarrollo, páginas web, aplicaciones y servidores, gestión del código fuente, la minimización de datos, etc. - CNIL. (2020). *GDPR Guide for Developers*. Recuperado de: https://bit.ly/3flUwup.

[57] 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 (BOE núm. 17, de 19 de enero de 2008).

información sobre las medidas de seguridad de la información en relación con la protección de datos personales[58].

El artículo 32 del RGPD contempla ciertos factores variables a la hora de aplicar medidas técnicas y organizativas, tales como el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad para los derechos y libertades de las personas físicas. Así, se recogen medidas como la seudonimización y el cifrado de datos, y el establecimiento de sistemas de restauración de la disponibilidad de la información, entre otras. Algunas de estas medidas serán aplicables cuando el alto riesgo para los derechos y libertades de los interesados así lo recomiende, pudiéndose modular las demás en función de tal nivel de riesgo.

A continuación se recomendarán medidas que, junto a las medidas técnicas y organizativas que serán abordadas en el apartado 6 del presente informe, dedicado a la seguridad de la información, permitirán rebajar el nivel de riesgo inicial detectado.

5.4.1. Acceso a *H&TeHealth* y creación de cuentas

La aplicación no requerirá de ninguna clase de proceso de instalación, ya que se tratará de una aplicación web. Una vez se tenga el acceso al software, este podrá ser utilizado en cualquier tipo de navegador.

Desde la perspectiva de los usuarios pacientes, existe un proceso de registro y acceso único. Es recomendable que en el momento en que el usuario accede a la aplicación por primera vez se muestren las Condiciones de uso citadas en el apartado 4 del presente informe, sobre Sociedad de la Información, además del resto de la información debida citada en aquél en términos de información legal y contratación.

Se recomienda que los usuarios queden perfectamente identificados y autenticados al acceder a la aplicación, sin perfiles genéricos, de manera que cada usuario tenga sus propias claves de acceso personalizadas.

En este punto se recomienda establecer medidas adicionales tales como la opción de que los usuarios puedan establecer plazos para la modificación de sus contraseñas

[58] Informe del Gabinete Jurídico de la AEPD Nº2009/0467, de 29 de enero de 2010. Recuperado de: https://bit.ly/2YxMRm5.

anualmente, como mínimo; así como el bloqueo de cuentas en casos de accesos erróneos reiterados a las cuentas de usuarios por la introducción de contraseñas incorrectas.

Asimismo, se recomienda establecer un sistema de doble validación (doble *opt-in*) mediante el que cada usuario recibirá un correo electrónico de confirmación en forma de notificación de su registro en la aplicación, por el que el usuario podrá ratificar su deseo de registrarse en *H&TeHealth* y que la dirección es correcta[59]. En este sentido, se propone un texto como el siguiente para la notificación vía correo electrónico:

"*Este correo electrónico es enviado para validar tu cuenta en H&TeHealth. Si deseas confirmar tu registro, haz clic en el este link. Si no eres el destinatario de este correo electrónico o no deseas confirmar tu registro, no hagas nada, tras siete días se procederá a borrar tus datos. Puedes ponerte en contacto con nosotros escribiéndonos a clientes@h&thospitales.com.*"

En relación con el tratamiento de datos de categoría especial, como los relativos a la salud de los usuarios, será necesario registrar el acceso a tales datos haciendo constar que el usuario de H&T ha accedido, la hora, el tipo de acceso llevado a cabo y la autorización o no a este.

Se recomienda que la información de este registro de accesos se conserve durante todo el tiempo que el usuario permanezca registrado en la aplicación y, tras su eventual baja, hasta un plazo de 5 años en modalidad de bloqueo (véase apartado 5.4.4.).

5.4.2. Recogida y uso de datos

Con carácter previo, cabe destacar que el Responsable del tratamiento debe informar a los usuarios interesados acerca de la recogida de datos que se realizará en, en este caso, la aplicación, y el uso que se les dará a aquéllos. Para informar a los usuarios acerca de los tratamientos que se describirán a continuación, se debe facilitar, tal y como establece la AEPD[60], lo siguiente:

[59] El principio de Opt-in fue introducido por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DOCE núm. L 201, de 31 de julio de 2002), como necesidad de contar con el consentimiento previo del destinatario de comunicaciones comerciales por correo electrónico, salvo supuestos de relación contractual anterior y no oposición.

[60] AEPD. (Septiembre de 2018). *Informe sobre políticas de privacidad en Internet*. Recuperado de: https://bit.ly/37tQhdw.

i. Identidad y datos de contacto del Responsable y, en su caso, de su representante.
ii. Contacto del Delegado de Protección de Datos (esta cuestión será tratada en el apartado 5.7 del presente informe).
iii. Categorías de datos que serán recogidos y tratados.
iv. Finalidades del tratamiento.
v. Base legitimadora del tratamiento.
vi. Derecho a retirar el consentimiento en cualquier momento, para aquellos tratamientos basados en aquél.
vii. Destinatarios de los datos recogidos.
viii. Transferencias internacionales de datos, en su caso.
ix. Plazo de conservación de los datos.
x. Posibilidad de ejercer los derechos de protección de datos.
xi. Posibilidad de presentar una reclamación ante la autoridad de control.
xii. Decisiones automatizadas, en su caso.

La información deberá ser concisa, transparente, de fácil acceso y con lenguaje claro y sencillo, lo que reforzará el sistema de bases de legitimación de los tratamientos. Así, en el mismo momento de la solicitud de los datos es recomendable mostrar un aviso de privacidad de primera capa que muestre la información básica del tratamiento y que enlace con la Política de Privacidad, la segunda capa informativa, en la que se vuelque la información completa sobre el tratamiento (disponible en el **Anexo IV**).

De este modo, se recomienda la elaboración y disposición de una **Política de Privacidad de la aplicación** (disponible en el **Anexo IV** del presente informe) que informe a los usuarios pacientes acerca de los tratamientos de datos realizados en *H&TeHealth*.

Asimismo, se recomienda que el Chatbot, como funcionalidad específica y de uso potestativo en la aplicación, que presenta particularidades en el tratamiento de datos tales como la interacción entre usuario persona física e IA, cuente con una **Política de Privacidad propia** (disponible en el **Anexo V** del presente informe).

Finalmente, se recomienda que la información sea presentada **"por capas"**, con el fin de lograr un equilibrio entre el deber de informar y la evitación del cansancio informativo en los usuarios de la aplicación.

A continuación se analizarán las diversas formas en que se recogerán los datos en *H&TeHealth*, con sus respectivas finalidades y bases de legitimación, así como la propuesta de información por capas citada.

5.4.2.1. Contacto

En la aplicación existirá un formulario mediante el que el usuario podrá ponerse en contacto con el titular y Responsable del tratamiento, H&T, para formular dudas, quejas o sugerencias de cualquier índole relacionadas con la aplicación y los servicios.

Los datos que en tal caso serán objeto de tratamiento serán de carácter identificativo y de contacto, con la finalidad de dar trámite a la duda, queja o sugerencia del usuario, gestionarla y darle una respuesta en un plazo razonable. En tal caso, el consentimiento del usuario se conforma como la base de legitimación del tratamiento de datos relativo al establecimiento de contacto con el Responsable en *H&TeHealth* (art. 6.1.a del RGPD).

Con respecto del consentimiento, cabe destacar que este debe ser recabado para cada finalidad, y que debe consistir en un acto afirmativo claro. Así lo recoge la jurisprudencia, de forma que no se podrán disponer mecanismos que priven al usuario de la capacidad de expresar tal acto afirmativo, como las casillas marcadas por defecto[61], ya que el consentimiento debe conformarse como una manifestación de voluntad libre y para fines específicos, fuera de los desequilibrios de poder propios de relaciones viciadas por la coacción o ciertos tipos de presión, y fuera de condicionalidades[62]. De este modo, los tratamientos basados en el consentimiento deberán prever igualmente un mecanismo fácil para su revocación[63].

En cuanto al tratamiento denominado “Contacto”, se recomienda facilitar información básica sobre el tratamiento en una primera capa informativa, a la vista en el propio formulario de contacto de la aplicación, con el texto propuesto siguiente:

[61] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 1 de octubre de 2019 (asunto C-673/17). Disponible en: https://bit.ly/2YyHYZV.
[62] La AEPD recoge igualmente estas características del consentimiento del interesado en sus resoluciones, siendo especialmente prolija en este sentido en su actuación sancionadora contra algunas compañías de telecomunicaciones que no recaban el consentimiento de los usuarios adecuadamente. Algunas de las más recientes, una multa a Másmóvil de 60.000 euros (Procedimiento PS/00262/2019: https://bit.ly/3d2YWVs) y una de 2.500 euros a Vodafone (Procedimiento PS/00184/2019: https://bit.ly/37tYwX0).
[63] GT29. (28 de noviembre de 2017). *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* (WP 259). Recuperado de: https://bit.ly/37vCHGU.

"*Trataremos tus datos para ponernos en contacto contigo a través del número de teléfono o dirección de correo electrónico que nos indiques, con el fin de resolver tus dudas o cuestiones que desees plantearnos por medio del presente formulario y, si lo deseas, para recibir comunicaciones periódicas con novedades, promociones y noticias de H&T Hospitales.*

Puedes ejercer tus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento escribiéndonos a rgpd@h&thospitales.com. Más información en nuestra Política de Privacidad."

Con este mensaje se estará informando al usuario acerca del tratamiento de sus datos y se le estará dando la posibilidad de acudir a la segunda capa informativa, la Política de Privacidad, mediante enlace, que le mostrará información más específica, si lo desea.

Por su parte, el acto expreso que conformará el consentimiento del usuario puede ser el mero hecho de que este haga clic en el botón "*Enviar*" del formulario de contacto, una vez mostrada la primera capa informativa con acceso directo a la segunda, de forma que no sería necesario incluir casillas de verificación para asegurarse de que el usuario ha leído la política de privacidad de H&T.

5.4.2.2. Registro

La aplicación permitirá registrarse en ella, lo que dará acceso a la interacción con el Chatbot y a la contratación del servicio de teleconsultas de *H&TeHealth*.

Los datos necesarios para completar el registro, con independencia de la posterior contratación o no, serán de carácter identificativo y de contacto, nuevamente. En este caso, la base de legitimación adecuada será la ejecución de un contrato en el que el interesado usuario es parte (art. 6.1.b del RGPD).

Cabe destacar que esta base de legitimación responde a que el registro en aplicaciones y plataformas de Internet supone la génesis de un contrato atípico de adhesión entre el Usuario y el titular de aquéllas del que se derivan derechos y obligaciones, generalmente recogidos en las Condiciones de Uso anteriormente citadas[64]. De esta manera, el

[64] Cuena Casas, M. (28 de febrero de 2019). Los riesgos para los consumidores y usuarios en la contratación a través de plataformas intermediarias en línea. *Hay Derecho – Expansión*. Recuperado de: https://bit.ly/386T0Ki.

incumplimiento de tal contrato deriva en consecuencias contractuales tales como la suspensión o cierre de cuentas personales de usuarios que incumplen, lo que supone en última instancia la resolución de este contrato particular.

En cuanto al registro en *H&TeHealth*, se recomienda facilitar información básica sobre el tratamiento en una primera capa informativa, a la vista en el propio formulario de registro de la aplicación, con el texto propuesto siguiente:

"*Trataremos tus datos para gestionar tu registro como usuario en H&TeHealth y prestarte los servicios ofrecidos en la aplicación.*

Puedes ejercer tus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento escribiéndonos a rgpd@h&thospitales.com. Más información en nuestra Política de Privacidad."

Con este mensaje se estará informando al usuario acerca del tratamiento de sus datos y se le estará dando la posibilidad de acudir a la segunda capa informativa, la Política de Privacidad de la aplicación, mediante enlace, que le mostrará información más específica, si así lo desea.

En este caso se recomienda habilitar un sistema de casillas de verificación por medio del cual el usuario pueda manifestar haber leído y comprendido, por un lado, la Política de Privacidad; y, por otro, las Condiciones de Uso de la aplicación (véase **apartado 4.2.1** del presente informe); como paso previo obligatorio para proceder a completar el proceso de registro en la aplicación.

5.4.2.3. Teleconsultas

Los usuarios registrados podrán contratar el servicio de teleconsultas de la aplicación. Los datos que se recabarán con el fin de gestionar la fijación de teleconsultas y prestar este concreto servicio de telemedicina serán, en el momento de la contratación, de carácter identificativo, de contacto y bancarios; y, en el momento de la prestación en sí, relativos a la salud y demás características del usuario paciente, que se transmitirán en el curso de la consulta en línea por videoconferencia, en cualquier tipo de soporte de datos como fotografías, documentos, informes, radiografías, etc.

En tal caso, la base de legitimación del tratamiento vuelve a ser la ejecución de un contrato en el que el usuario paciente es parte (art. 6.1.b del RGPD).

Esta base responde a que, en lo que respecta a la dispensa de servicios sanitarios, los médicos o centros sanitarios no necesitan recabar el consentimiento de los pacientes para el tratamiento de datos de salud si estos van a utilizarse para fines de medicina, diagnóstico médico, prestación de asistencia sanitaria, etc.[65]

En cuanto a la contratación de teleconsultas, se recomienda facilitar información básica sobre el tratamiento en una primera capa informativa, a la vista en el propio formulario de contratación de la aplicación, con el texto propuesto siguiente:

"*Trataremos tus datos para concertar una consulta online, facilitarte los datos de acceso y conexión a la misma y obtener información básica para prepararla.*

Puedes ejercer tus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento escribiéndonos a rgpd@h&thospitales.com. Más información en nuestra Política de Privacidad."

Con este mensaje se estará informando al usuario acerca del tratamiento de sus datos y se le estará dando la posibilidad de acudir a la segunda capa informativa, la Política de Privacidad, mediante enlace, que le mostrará información más específica, si así lo desea.

En este caso se recomienda habilitar un sistema de casillas de verificación por medio del cual el usuario pueda manifestar haber leído y comprendido, por un lado, la Política de Privacidad; y, por otro, las Condiciones Generales de Contratación aplicables a la contratación del servicio de teleconsultas (véase **apartado 4.2.2** del presente informe); como paso previo obligatorio para proceder a completar el proceso de contratación.

La información sobre el tratamiento de datos para este fin deberá verse complementada, en el momento de la contratación, con aquella información relativa a las características y eventuales consecuencias del servicio sanitario prestado, en aras de obtener el consentimiento informado del usuario en lo que respecta a ser tratado mediante un sistema de teleconsultas como el de H&TeHealth, en el ámbito estrictamente sanitario (véase **apartado 3.3.1** del presente informe).

[65] AEPD. (2019). *Guía para pacientes y usuarios de la Sanidad*. Recuperado de: https://bit.ly/3i6maOy.

5.4.2.4. Chatbot

Los usuarios registrados en la aplicación también podrán hacer uso de la funcionalidad de Chatbot ofrecida en *H&TeHealth*, por medio de la interacción con el mismo. Se tratará de una funcionalidad de uso potestativo, no necesaria para la contratación del servicio de teleconsultas, aun a pesar de que tras completar el cuestionario del Chatbot el usuario tendrá la posibilidad de acudir directamente a la página de contratación de teleconsultas de la aplicación. El objetivo del Chatbot será, mediante la interacción con el usuario, elaborar una recomendación de elección de facultativo de H&T en función del cuadro sintomatológico que el usuario presenta en virtud de la información que suministrará y, así, recomendar la contratación de una teleconsulta, en su caso.

A tal fin, se estarán recogiendo datos sobre características personales del interesado, sus circunstancias laborales y sociales y, sobre todo, datos relativos a su salud.

En tal caso, la base de legitimación del tratamiento se sustentará en el consentimiento explícito del usuario (art. 9.2.a del RGPD), ya que el Chatbot se trata de una funcionalidad que no entra dentro de lo que denominamos servicio sanitario o de diagnóstico oficial[66], por lo que el consentimiento explícito del usuario para las finalidades específicas del tratamiento de Chatbot será lo que permita tratar datos de salud en este caso. Es el usuario el que decide interactuar con el bot y facilitar a este datos de diversa índole, sin que no hacerlo sea obstáculo para contratar una teleconsulta.

En lo que respecta al uso del Chatbot, se recomienda incluir información básica sobre el tratamiento en una primera capa informativa, a la vista al acceder a la funcionalidad del Chatbot y antes de que se proceda a iniciar la interacción, con el texto propuesto siguiente:

"*Trataremos tus datos con el fin de elaborar una recomendación de elección de facultativo en función de tu posible cuadro sintomatológico, así como para redirigirte a nuestro formulario de contratación de teleconsulta, si fuera de tu interés.*

Puedes ejercer tus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento escribiéndonos a rgpd@h&thospitales.com. Más información en nuestra Política de Privacidad."

[66] ECIJA & Chatbot Chocolate. (2018). *Guía legal chatbots: aspectos jurídicos y de mercado*. Recuperado de: https://bit.ly/2ULLhfv.

Con este mensaje se estará informando al usuario acerca del tratamiento de sus datos y se le estará dando la posibilidad de acudir a la segunda capa informativa, la Política de Privacidad específica del Chatbot, que le mostrará información más específica sobre el tratamiento de sus datos, si así lo desea.

El acto expreso que conformaría el consentimiento del usuario podría ser el mero hecho de que este haga clic en el botón "*Comenzar*" o "*Acepto*" de la página del Chatbot en la aplicación como paso previo a comenzar con la interacción, una vez mostrada la primera capa informativa con acceso directo a la segunda, de forma que no sería necesario incluir casillas de verificación para asegurarse de que el usuario ha leído la política de privacidad específica del Chatbot.

5.4.2.5. Marketing

Desde *H&T Hospitales* se ha planteado la posibilidad de utilizar los datos de contacto de los usuarios con el fin de remitirles comunicaciones comerciales por correo electrónico acerca de los servicios de H&T, novedades, etc.

En este sentido, cabe destacar que la regla general es que se prohíben las comunicaciones publicitarias de esta índole por vía electrónica, tal y como dispone el artículo 21.1 de la LSSI, cuando no hayan sido previamente solicitadas o autorizadas por sus destinatarios. La excepción a esta regla es que exista una relación contractual previa con el destinatario, con la obtención de los datos de forma previa y lícita, y que las comunicaciones remitidas en virtud de tal relación previa se refieran a servicios de H&T similares a los inicialmente contratados por el destinatario.

Por su parte, el artículo 23 de la LOPDGDD, al hablar de los sistemas de exclusión publicitaria, establece que en supuestos de realización de comunicaciones de mercadotecnia directa se deberán consultar los sistemas de exclusión publicitaria que sean susceptibles de afectar a tal actuación, de forma que si el destinatario de las comunicaciones ha manifestado su oposición al envío de estas mediante su adhesión a alguno de estos sistemas, no deberán enviársele tales comunicaciones[67].

[67] En España, existe un fichero de exclusión publicitaria gestionado por la Asociación Española de la Economía Digital, denominado como la "*Lista Robinson*", accesible en https://www.listarobinson.es/.

En el caso de los destinatarios que no hayan contratado previamente con H&T, la base de legitimación debe sustentarse en el consentimiento del usuario (art. 6.1.a del RGPD). En otro caso, como se ha indicado en las excepciones del artículo 21 de la LSSI, cabría una base legitimación fundada en el interés legítimo del Responsable del tratamiento (art. 6.1.f del RGPD), pero dejando lugar a la oposición por parte del usuario en todo caso.

En este sentido, se recomienda que en el momento en que se proceda a recoger los datos (por ejemplo, en los formularios de contacto, de contratación de teleconsultas, etc.) se incluya el siguiente texto propuesto:

"*Deseo recibir comunicaciones de H&T Hospitales por medios electrónicos*".

Se recomienda que el usuario pueda prestar su consentimiento mediante una casilla de verificación junto al texto propuesto, sin premarcar y potestativa en todo caso para el trámite en cuestión que esté realizando el usuario, de manera que este pueda marcarla si efectivamente desea recibir comunicaciones comerciales.

Asimismo, se recomienda implantar un mecanismo de baja del sistema de envío de comunicaciones de fácil acceso para el usuario, mediante, por ejemplo, el ofrecimiento de una dirección de correo electrónico a la que se pueda comunicar la oposición a la recepción de las comunicaciones, o alguna clase de enlace de baja automática en las propias comunicaciones comerciales enviadas por medios electrónicos.

El texto que se propone para las comunicaciones, en este sentido, es el siguiente:

"*Esta comunicación ha sido remitida por H&T Hospitales, S.A., con NIF A12345678 y domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid). Podrás ejercer tus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento en cualquier momento, escribiéndonos a rgpd@h&thospitales.com. Asimismo, si no deseas recibir más comunicaciones como esta, escríbenos a la misma dirección de correo electrónico o haz clic en este enlace.*"

5.4.2.6. Perfilado estadístico

Finalmente, se ha planteado la posibilidad, desde *H&T Hospitales*, de elaborar un perfilado con fines estadísticos a partir de los datos obtenidos en las interacciones del Chatbot con los usuarios.

El perfilado estadístico surge como confluencia de tres aspectos: el tratamiento automatizado, los datos personales y la evaluación de las personas físicas, con el fin de crear nuevos datos en forma de deducciones estadísticas[68], estableciendo correlaciones que logren crear nueva información interpretable, mediante la inferencia[69]. Se trata de técnicas de Big Data que el artículo 22 del RGPD no prohíbe, pero que supedita al consentimiento explícito del interesado en un caso como el de *H&TeHealth*, en virtud del artículo 9.2.a del RGPD por incluir datos relativos a la salud. Por lo tanto, los interesados tendrán derecho a no ser objeto de elaboración de perfiles. Eso sí, este derecho concurrirá cuando el perfilado comporte efectos jurídicos para el interesado o le afecte de modo similar[70].

Habida cuenta de lo anterior, se recomienda que los datos recabados por el Chatbot que vayan a ser utilizados con fines de perfilado estadístico sean anonimizados y, así, lograr la no aplicación del RGPD en este caso (véase el **apartado 5.4.4** del presente informe). En concreto, se recomienda que los datos sean previamente anonimizados, agregados y extrapolados, antes de proceder a su tratamiento con fines estadísticos.

Asimismo, se recomienda garantizar la irreversibilidad de la anonimización de los datos utilizados, de forma que no se permita la identificación de los interesados titulares de los datos de carácter personal y pueda acreditarse la disociación de aquéllos, sin dejar lugar a inferencias. Los algoritmos de cifrado serán útiles en este proceso (véase **apartado 6.3.2.2** del presente informe).

En caso de que los datos no vayan a pasar por un proceso de anonimización, se deberá recabar el consentimiento explícito de los usuarios interesados para la finalidad específica de perfilado con fines estadísticos. En tal caso, lo recomendable sería incluir el siguiente texto, junto a una casilla de verificación sin premarcar mediante la que el usuario pueda prestar su consentimiento mediante acto expreso:

"*Deseo que mis datos sean utilizados para la elaboración de perfiles con fines estadísticos.*

[68] Reyes Rico, L. (13 de agosto de 2019). Límites de la normativa de protección de datos a la creación de perfiles con fines comerciales. *LegalToday*. Recuperado de: https://bit.ly/3884A84.
[69] Gil, E. (2015). Big data, privacidad y protección de datos. *Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado*. Recuperado de: https://bit.ly/2VqPXrk.
[70] AEPD. (2017). *Código de buenas prácticas en protección de datos para proyectos Big Data*. Recuperado de: https://bit.ly/31pF64Q.

Podrás ejercer tus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento en cualquier momento, escribiéndonos a rgpd@h&thospitales.com. Asimismo, podrás revocar tu consentimiento en cualquier momento escribiéndonos a la misma dirección de correo electrónico o haciendo clic en este enlace."

5.4.3. Supresión y bloqueo de datos

El artículo 32 de la LOPDGDD establece que cuando se proceda a la rectificación o supresión de los datos, el Responsable del tratamiento deberá bloquearlos.

La propia Ley define el bloqueo, como la identificación y reserva de datos adoptando medidas técnicas y organizativas para impedir su tratamiento hasta que sea necesaria la puesta a disposición de aquéllos a órganos jurisdiccionales, Administraciones Públicas y demás autoridades competentes, en su caso, para la depuración de responsabilidades derivadas del tratamiento durante el plazo de prescripción de tales responsabilidades. Una vez agotado dicho plazo, sí deberá procederse a la destrucción y borrado total de los datos, en todo caso.

Se recomienda que H&T cuente con alguna herramienta que le permita descargar la información para almacenarla debidamente bloqueada en su sistema, cuando corresponda.

Así, en relación con los tratamientos de datos indicados en el apartado anterior, se recomiendan los siguientes plazos de conservación, tras cuyo agotamiento deberá procederse a su bloqueo:

i. Contacto: plazo de 1 año desde la recogida de los datos.
ii. Registro: para la ejecución del contrato que es la base de legitimación de este tratamiento, los datos se conservarán durante todo el tiempo en que el usuario permanezca registrado en *H&TeHealth*.
iii. Teleconsultas: los datos relativos a la salud que sean incorporados a la Historia Clínica del usuario paciente, y demás documentación clínica, deberán ser conservados al menos durante 5 años desde la fecha de alta de cada proceso asistencial, en virtud del artículo 17 de la Ley de autonomía del paciente.
iv. Chatbot: plazo de 1 año desde la recogida de los datos. Para aquellos casos en que el usuario no sólo interactúe con el bot sino que, adicionalmente, contrate el servicio de

teleconsulta, se recomienda el plazo de conservación asociado a la relación contractual en tal caso. Para el supuesto en que los datos sean adicionalmente tratados para perfilado con fines estadísticos, sin anonimización, se podrán tratar los datos mientras el usuario interesado no revoque su consentimiento.

v. Marketing: los datos se conservarán durante todo el tiempo en que el usuario permanezca suscrito al sistema de envío de comunicaciones comerciales de la aplicación.
vi. Perfilado estadístico: en tanto en cuanto los datos estén irreversiblemente anonimizados, la normativa de protección de datos no será aplicable en términos de plazos de conservación.

5.4.4. Seudonimización y anonimización

En la medida en que los datos de usuarios pacientes de *H&TeHealth* se puedan ver comprometidos, conviene hablar de dos conceptos fundamentales en la privacidad desde el diseño: la seudonimización y la anonimización.

Por un lado, la seudonimización consiste en el tratamiento de datos personales que no puedan ser atribuidos a una determinada persona física sin que, para ello, se deba utilizar información adicional, siempre que tal información adicional figure por separado y esté sujeta a medidas destinadas a garantizar su confidencialidad. En la seudonimización persiste la probabilidad de identificar a la persona física de forma indirecta, y se utilizan técnicas como el cifrado (véase **apartado 6.3.2.2** del presente informe).

Por otro lado, la anonimización consiste en el proceso por el que se elimina la posibilidad de identificar a una persona física. Los datos anonimizados, siempre que lo sean irreversiblemente, quedan fuera del ámbito de aplicación de la normativa de protección de datos. Una anonimización adecuada garantiza la imposibilidad de vincular cualquier dato a una persona física, teniendo en cuenta los riesgos básicos de cualquier técnica de anonimización: la singularización (posibilidad de extraer registros de conjuntos de datos que identifiquen a una persona), la vinculabilidad (capacidad de vincular dos registros de una base de datos, o varias, sobre un interesado) y la inferencia (posibilidad de deducir el valor de un atributo a partir de los valores de otros)[71].

[71] GT29. (10 de abril de 2014). *Dictamen 05/2014 sobre técnicas de anonimización* (WP 216). Recuperado de: https://bit.ly/2AzDQ42.

No obstante, debe tenerse en cuenta, de cara a los interesados, que los datos deben ser conservados en un formato identificable con el fin de que aquéllos puedan ejercer sus derechos de protección de datos ante el Responsable del tratamiento[72].

5.5. Ejercicio de derechos

El Considerando 11 del RGPD determina que la protección de datos requiere del refuerzo y especificación de los derechos de los interesados y las obligaciones con respecto de estos por parte de quienes tratar y determinan el tratamiento de datos.

El abanico de derechos en materia de protección de datos que asisten a los interesados es el siguiente:

i. **Acceso:** derecho a obtener confirmación de si se tratan datos, a acceder a tales datos y a obtener información sobre su tratamiento.
ii. **Rectificación:** derecho a rectificar los datos inexactos.
iii. **Limitación del tratamiento:** derecho a que los datos sean reservados y utilizados sólo con el consentimiento del interesado para formular reclamaciones, ejercer derechos de protección de datos o por razones de interés público.
iv. **Portabilidad:** derecho a obtener una copia de los datos y a que esta sea remitida a otro responsable del tratamiento.
v. **Oposición:** derecho a oponerse a que el Responsable realice tratamientos sobre sus datos, salvo casos de interés legítimo imperioso de aquél.
vi. **Supresión:** derecho a que los datos sean suprimidos, bajo ciertas circunstancias (datos innecesarios en relación con las finalidades para las que fueron recabados; retirada del consentimiento en tratamientos basados únicamente en el mismo; oposición al tratamiento; tratamiento ilícito de los datos; obligación legal de supresión; y/o datos obtenidos en relación con la oferta de servicios de la sociedad de la información).

En este sentido, H&T debe facilitar a los usuarios interesados de *H&TeHealth* la información indicada con anterioridad, con la indicación de los medios de comunicación habilitados para que aquéllos puedan ejercer sus derechos de protección de datos de modo

[72] Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera), de 7 de mayo de 2009 (asunto C-553/07). Disponible en: https://bit.ly/3e2nFL6.

sencillo y gratuito[73]. Ante una solicitud de ejercicio de derechos, se deberá dar respuesta a esta en el plazo de 1 mes desde su recepción por parte de H&T[74].

Se recomienda que, en la medida en que todos los datos tratados en la aplicación lo serán por medios electrónicos, los medios proporcionados para facilitar el ejercicio de los derechos descritos sean igualmente electrónicos.

En este sentido, la indicación de una dirección de correo electrónico a la que dirigir las solicitudes de ejercicio bastaría, como se ha puesto de manifiesto en los textos legales de los anexos del presente informe y en los avisos informativos de primera capa indicados con anterioridad.

Asimismo, a efectos de lograr una mayor rapidez en la gestión de solicitudes, se recomienda facilitar el acceso directo a sus datos personales a los usuarios interesados de la aplicación, con el fin de evitar solicitudes de acceso y derivar recursos a eventuales solicitudes de ejercicio de otros derechos.

Asimismo, se recomienda que, en el caso de que existan dudas sobre la identidad de la persona física que solicita el ejercicio de derechos, se le solicite adicionalmente una acreditación de identidad (por ejemplo, copia de un documento oficial de identidad como el DNI). Esto redundará en la protección de datos y la seguridad de la información, ya que se estarán evitando accesos no autorizados a los datos en caso de que la persona no sea quien dice ser.

5.6. Encargo del tratamiento

Es posible que *H&T Hospitales*, como Responsable del tratamiento en *H&TeHealth*, requiera de terceras entidades o profesionales para que realicen ciertas actuaciones o presten alguna clase de servicio, lo que conllevará, en todo o en parte, el tratamiento de datos.

Durante las conversaciones previas a la realización del presente informe, desde H&T se planteó la posibilidad de que el desarrollo y posterior mantenimiento de la aplicación

[73] El artículo 12 del RGPD permite cobrar un canon razonable, basado en costes administrativos, ante solicitudes reiteradas de ejercicio de derechos, o en casos de solicitudes manifiestamente infundadas o excesivas.

[74] Este plazo puede verse ampliado hasta en dos meses más, en función de la complejidad y el número de solicitudes recibidas, siempre que se informe de ello al interesado explicando los motivos de la dilación

fuera externalizado a una empresa especializada, es decir, que se encargara la realización de tales actividades. En tal caso, nos encontraríamos ante un encargo del tratamiento en el que el prestador de los servicios estaría tratando datos de responsabilidad de H&T por cuenta de esta última. En este sentido, la relación entre Responsable y Encargado debe formalizarse en un contrato o acto jurídico que genere una vinculación entre ambas partes, por escrito, y que contenga, al menos, todo lo establecido por el artículo 28 del RGPD, a saber: actuación del Encargado bajo las instrucciones del Responsable, compromiso de confidencialidad, asistencia al Responsable en el cumplimiento de atención a las solicitudes de ejercicio de derechos por parte de los interesados, etc.

Cabe destacar que a la hora de elegir un Encargado del tratamiento, el Responsable debe elegir sólo a aquellos que garanticen de forma suficiente la aplicación de medidas técnicas y organizativas apropiadas para que el tratamiento de datos encargado se adapte a los requisitos del RGPD, protegiendo en todo caso los derechos de los interesados.

Es recomendable documentar el proceso de elección de proveedores, con los motivos de elección o no elección de cada uno, en una muestra más de diligencia y responsabilidad proactiva por parte de H&T con respecto de los datos tratados en su organización.

En este sentido, el Considerando 78 del RGPD establece que "*ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones*", por lo que en el caso de que H&T decida finalmente externalizar esta actividad en un proveedor de software, deberá desempeñar un papel activo en el aseguramiento de los principios de la protección de datos en el flujo de estos entre Responsable y eventual Encargado.

El objetivo de dicha proactividad es conocer cuestiones tales como, por ejemplo, la subcontratación por parte del Encargado de todas o alguna de las actividades que entrañará el servicio prestado, ya que existe la posibilidad de limitar tal cuestión en el contrato de encargo del tratamiento. En todo caso, no obstante, los subcontratistas, como subencargados del tratamiento, "*deben estar sujetos a las mismas condiciones y en la*

misma forma que el encargado del tratamiento en lo referente al adecuado tratamiento de los datos personales"[75].

En el marco del proceso de elección de proveedores, se recomienda remitir comunicaciones a todos ellos solicitando información acerca de su nivel de cumplimiento normativo en términos de privacidad, junto a un documento de comprobación en forma de lista de verificación, *checklist* (se aporta un modelo de cuestionario para encargados del tratamiento en el **Anexo VI** del presente informe).

Resulta igualmente recomendable llevar a cabo un registro actualizado de todos los Encargados del tratamiento de H&T, por medio del cual se pueda monitorizar la estructura de los tratamientos de datos llevados a cabo en la organización.

Finalmente, cabe destacar el hecho de que *H&T Hospitales*, como Responsable del tratamiento, mantiene una facultad de supervisión sobre el Encargado en un régimen de responsabilidad por culpa *in vigilando*[76] derivado de la responsabilidad *in eligendo* del hecho de que es el Responsable el que debe elegir sólo a aquellos Encargados que presenten garantías suficientes, como se ha indicado. Las consecuencias de esta clase de responsabilidad descansan sobre el vínculo causal existente entre Responsable y Encargado que, como dispone el artículo 1903 del Código Civil, implica la infracción del deber de cuidado que es reprochable al empresario en la selección de dependientes o en el control de la actividad de estos. Concurre, por tanto, una derivación de responsabilidad "*más allá del autor propio del evento dañoso, creando un litisconsorcio pasivo necesario entre la persona causante del daño y aquella otra que tenía una directa obligación de vigilar que el causante del daño debía tener una conducta correcta en su actuación*"[77]. Una posición pasiva es precisamente lo que genera responsabilidad, lo cual se aleja de la responsabilidad proactiva exigida por el RGPD.

La jurisprudencia avala igualmente este régimen de responsabilidad *in vigilando*, describiendo supuestos perfectamente aplicables al ámbito de la protección de datos, en los que existe "*un nexo entre dos personas caracterizado por la existencia en una de ellas*

[75] Autoridad Catalana de Protección de Datos. (2019). *El encargado del tratamiento en el Reglamento General de Protección de Datos (RGPD)*. Recuperado de: https://bit.ly/2YIy4Fp.
[76] Álvarez Hernando, J. (2011). *Guía práctica sobre Protección de datos: cuestiones y formularios*. Madrid: Lex Nova.
[77] Magro Servet, V. (2013). Responsabilidad por culpa in vigilando. *Revista de Jurisprudencia LEFEBVRE-El Derecho, nº2*. Recuperado de: https://bit.ly/3dqW7Op.

de facultades de impartir órdenes e instrucciones a la otra" (STS 1465/2009)[78], como ocurre en el encargo del tratamiento llevado a cabo por cuenta y bajo las instrucciones del Responsable.

De este modo, el Responsable se erige como garante último ante los interesados del cumplimiento de los deberes de protección de datos, algo que H&T deberá tener en cuenta especialmente en casos en que se contrate con proveedores de servicios en la nube, Plataforma como Servicio (*Platform as a Service, PaaS*), Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) o Software como Servicio (*Software as a Service, SaaS*), cuya prestación implicará el tratamiento de datos por cuenta del Responsable en casi todos los supuestos[79] y tal será el caso de H&T si decide externalizar el desarrollo y el mantenimiento de la aplicación *H&TeHealth*.

H&T debe asumir los eventuales daños ocasionados como consecuencia de un tratamiento de datos del cual ha definido sus fines y medios por sí misma, sin perjuicio de que el tratamiento termine encargándose. En su caso, se habrá de depurar responsabilidades y concurrirá la facultad de repetición.

5.7. Delegado de Protección de Datos

El Delegado de Protección de Datos (DPD) es un profesional que se encarga de asesorar a la organización en todo lo relacionado con el cumplimiento de la normativa de protección de datos, de supervisar su cumplimiento a nivel interno y de actuar como punto de contacto con la autoridad de control correspondiente. Cabe destacar que existe cierta flexibilidad en su régimen: su dedicación puede ser completa o parcial, y puede designarse un DPD interno o externo a la organización. El único requisito que debe garantizarse en todo caso en lo que respecta al Delegado es que este cuente con los suficientes conocimientos especializados en materia de privacidad y su práctica, que cuente con medios a tal fin y que se le facilite la autonomía funcional necesaria para llevar a cabo su tarea.

Lo propio del DPD es que pueda participar de forma adecuada y oportuna en todas las cuestiones relacionadas con la protección de datos de la organización, sin instrucciones

[78] Sentencia del Tribunal Supremo 1465/2009, de 17 de marzo de 2009. Disponible en: https://bit.ly/2Vc9s6N.
[79] Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales: el remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil*, Vol. V, (nº4), pp. 53-87.

en lo que respecta al desempeño de sus funciones, marcando un claro carácter protagónico y de independencia dentro de su actividad asesora y supervisora. Por tanto, la persona designada para ocupar esta posición estará implicada en cuestiones como el desarrollo de nuevos tratamientos o soluciones que, como *H&TeHealth*, entrañen aspectos sobre la protección de datos de carácter personal. El Delegado también estará presente en las acciones de formación continua llevadas a cabo en la organización, supuesto en el que será probable y preciso que sea el propio DPD quien diseñe el material formativo para la plantilla. La LOPDGDD, además, atribuye al Delegado un rol de mediador entre afectados y la autoridad de control, la AEPD, en supuestos de reclamaciones, por el que se trate de buscar soluciones antes de acudir a la vía administrativa ante la Agencia. El perfil del DPD requerirá, por tanto, de una serie de estándares profesionales de compleja consecución en la organización en que se incardine[80].

Por tanto, el análisis de esta figura con respecto de la aplicación *H&TeHealth* debe realizarse con la vista puesta en *H&T Hospitales* como organización responsable del tratamiento de los datos.

El artículo 37 del RGPD regula la designación del Delegado de Protección de Datos (DPD), indicando tres supuestos en que tal designación será preceptiva: (a) cuando el tratamiento sea llevado a cabo por autoridades u organismos públicos, (b) cuando las actividades del Responsable del tratamiento requieran de la observación habitual y sistemática de interesados a gran escala, y (c) cuando las actividades del Responsable del tratamiento consistan en el tratamiento a gran escala de categorías especiales de datos personales. Por su parte, el artículo 34 de la LOPDGDD recoge los tipos específicos de organizaciones que tienen la obligación de nombrar un DPD, a saber, entre otras: los colegios profesionales, los centros docentes, los establecimientos financieros de crédito, las entidades aseguradoras y, en lo que a H&T respecta, los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes (artículo 34.1.l) de la Ley).

Se recomienda a *H&T Hospitales* la designación de un Delegado de Protección de Datos a la vista de la normativa y las especialidades del tratamiento de datos analizadas en el

[80] Valín López, M. (2018). Apuntes sobre el Delegado de Protección de Datos y la Administración General de Euskadi. *Revista Vasca de Gestión de Personas y Organizaciones Públicas* (nº 14), pp. 92-105. Recuperado de: https://bit.ly/2VoJCNb.

presente informe, toda vez que la actividad principal de un hospital u hospitales es prestar atención sanitaria, independientemente de la modalidad de esta, sin que sea posible que se preste atención sanitaria segura y eficaz sin tratar datos relativos a la salud[81].

Entre las funciones que desempeñará el DPD y que recoge el artículo 39 del RGPD, podemos encontrar funciones desde la perspectiva del cumplimiento normativo (identificación de bases legitimadoras de tratamientos, contratación de encargados, diseño e implantación de políticas de privacidad, etc.), desde la de la relación con los interesados (diseño e implementación de políticas y medidas de información a los interesados, recepción y gestión de solicitudes de ejercicio de derechos, etc.), desde la de la seguridad (análisis de riesgos, procedimientos de gestión de violaciones de seguridad, etc.), desde la de la prevención (EIPD y medidas de protección desde el diseño y por defecto), así como desde la de la formación y la cooperación con la autoridad de control, como se ha indicado[82].

En el ámbito de la salud, a mayor abundamiento, el Delegado de Protección de Datos desempeña un papel esencial en tanto en cuanto se estarán tratando datos relativos a la salud, especialmente protegidos y sensibles, que requerirán de políticas, procedimientos y medidas adecuadas que evolucionen se adapten constantemente al desarrollo del tratamiento y las actividades de la organización. Asimismo, cabe esperar solicitudes de ejercicio de derechos por parte de usuarios pacientes de *H&TeHealth*, por la desconfianza que es susceptible de generar la transmisión de datos de salud a través de una aplicación, por lo que la intermediación de un DPD devendrá totalmente necesaria a efectos de gestión de solicitudes y eventuales reclamaciones ante la AEPD.

[81] GT29. (2016). *Directrices sobre los delegados de protección de datos (DPD)* (WP 243). Recuperado de: https://bit.ly/2NAbzgF.
[82] Villaseca, M. (2018). El delegado de protección de datos. *I+S: Revista de la Sociedad Española de Informática y Salud* (nº 127), pp. 21-23. Recuperado de: https://bit.ly/3i1XxCq.

6. Seguridad de la información

Como afirma el Considerando 1 de la Directiva NIS[83], "*las redes y sistemas de información desempeñan un papel crucial en la sociedad. Su fiabilidad y seguridad son esenciales para las actividades económicas y sociales*". De esta manera, entendemos por seguridad de las redes y de la información la capacidad de estos sistemas de resistir accidentes y acciones malintencionadas que puedan comprometer alguno o algunos de los requisitos indispensables en la valoración de la información, asociados a sus respectivas amenazas, a saber[84]:

i. Confidencialidad: revelación de la información a personas no autorizadas o que no necesiten conocerla.
ii. Integridad: modificación de la información por alguien no autorizado a tal fin.
iii. Autenticidad: información no auténtica.
iv. Trazabilidad: imposibilidad de rastrear quién ha accedido o modificado la información.
v. Disponibilidad: imposibilidad de acceso a la información por personas autorizadas cuando ello sea necesario.

El objetivo de este apartado es establecer una serie de protocolos en relación con la seguridad de la información partiendo de estos cinco requisitos, para garantizar este punto en *H&TeHealth*. Cabe aclarar que no existe la seguridad absoluta, de forma que debemos entender la seguridad como una función, como el conjunto de actividades dirigidas a identificar riesgos, eliminar vulnerabilidades, prever incidentes, limitar los efectos de estos, reparar los daños y recuperar las funcionalidades del sistema de información de la aplicación de la forma más rápida y menos dañina posible.

En España, el ENS[85] sirve de inspiración en cuanto a los principios y garantías básicas que debe reunir un sistema de información, aun a pesar de que se trata de un esquema

[83] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DOUE núm. L 194, de 19 de julio de 2016).
[84] Centro Criptológico Nacional. (2011). *Guía de Seguridad: Esquema Nacional de Seguridad, valoración de los sistemas*. Recuperado de: https://bit.ly/30XHoYN.
[85] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE núm. 25, de 29 de enero de 2010).

cuyo ámbito de aplicación se limita a las Administraciones Públicas. En este sentido, un SGSI deberá contemplar, al menos, las siguientes cuestiones:

i. Organización e implantación del proceso de seguridad.
ii. Análisis y gestión de los riesgos.
iii. Gestión de personal.
iv. Autorización y control de los accesos.
v. Seguridad por defecto.
vi. Integridad y actualización del sistema.
vii. Protección de la información almacenada y en tránsito.
viii. Registro de actividad.
ix. Incidentes de seguridad.

6.1. Identificación de activos y riesgos

A la hora de abordar los aspectos relacionados con la seguridad de un sistema de información como el de *H&TeHealth* identificando, en primer lugar, se deben identificar dos cuestiones fundamentales: cuáles son los activos del sistema y cuáles son los riesgos a los que se enfrentan. La evaluación del riesgo se conforma, una vez más, como un elemento fundamental en la seguridad de la información, con el posterior diseño y realización de la seguridad[86].

Entendemos los activos como aquellos componentes o funcionalidades del sistema de información que son susceptibles de ser atacados, con consecuencias para la organización: información en general, datos de carácter personal, equipos y demás recursos. Aunque pueden existir activos de diverso valor, el mínimo común denominador de todos ellos es que todos, en mayor o menor medida, presentan un interés para la organización.

Por su parte, entendemos los riesgos como las estimaciones del grado de exposición a que una amenaza se materialice sobre uno o más activos del sistema, causando daños a la organización[87].

[86] Organización para la Cooperación y el Desarrollo Económicos. (2002). *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad*. Recuperado de: https://bit.ly/2zGQUEl.
[87] Mujica, M. y Álvarez, Y. (2009). El Análisis de Riesgo en la seguridad de la información. *Publicaciones en Ciencias y Tecnología*, Vol. 4, nº2 (pp. 33-37).

La magnitud y el eventual efecto perturbador de un incidente se mide en función de factores sectoriales, y en el sector sanitario uno de estos factores puede ser el número de pacientes atendidos y tratados cada año por un prestador de servicios sanitarios, por ejemplo, tal y como indica el Considerando 28 de la Directiva NIS. En este sentido debe aclararse que un prestador de servicios sanitarios, público o privado, como *H&T Hospitales*, entra dentro del concepto de operador de servicios esenciales y, como tal, debe atenerse a unas obligaciones reforzadas en el ámbito de la seguridad de la información, que en esencia son la adopción de medidas adecuadas acordes con el nivel de riesgo afrontado y la notificación de incidentes de seguridad relevantes.

De esta manera, ante un incidente de seguridad en el sistema de información de H&T se deberán tener en cuenta dos parámetros fundamentales: el alcance de la afectación a la otra parte de la relación, en su caso; y el número de usuarios afectados que hayan utilizado la aplicación con base en el tráfico de datos previo. El impacto del incidente devendrá significativo cuando se haya dado una pérdida de autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados en *H&TeHealth* y los sistemas de H&T[88].

6.2. Seguridad de la información y protección de datos

El Considerando 63 de la Directiva NIS establece la relación existente entre la seguridad de la información y la protección de datos, dos materias que irán de la mano en múltiples ocasiones, ya que los datos de carácter personal formarán parte del sistema de información y podrán verse igualmente comprometidos como consecuencia de un incidente de seguridad en el sistema. El artículo 32 del RGPD, por su parte, como se ha indicado previamente en el presente informe, obliga a Responsables y Encargados del tratamiento a aplicar medidas técnicas y organizativas que garanticen "*un nivel de seguridad adecuado al riesgo*" del tratamiento.

De la transmisión de datos relativos a la salud que se llevará a cabo mediante las diversas funcionalidades *H&TeHealth* deriva, precisamente, la principal amenaza de la aplicación

[88] Reglamento de Ejecución (UE) 2018/151 de la Comisión, de 30 de enero de 2018, por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo (DOUE núm. L 26, de 31 de enero de 2018).

en términos de confidencialidad[89]. La Historia Clínica es el principal activo del sistema de información de la aplicación en lo que respecta a los datos de carácter personal[90], toda vez que, además, estaremos hablando de una Historia Clínica electrónica que se expone a las amenazas asociadas a la propia naturaleza del entorno digital.

La Historia Clínica electrónica, como registro cronológico de todos los acontecimientos de la salud de una persona física, presenta una serie de particularidades como es la ordenación determinada de la información, la uniformidad de documentos, la legibilidad, las pretendidas inalterabilidad y disponibilidad de su contenido y, como es lógico, el almacenamiento en soportes electrónicos[91]; particularidades que se convierten en objeto de protección del activo en términos de seguridad de la información: confidencialidad, integridad y disponibilidad de la información.

Además de las medidas que se han expuesto hasta ahora en el presente informe, será necesario blindar la aplicación y el sistema de H&T de manera que la Historia Clínica quede debidamente protegida frente a amenazas accidentales o volitivas, citadas con anterioridad. Asimismo, el conocimiento en el manejo de las TIC por parte del equipo de H&T y el efectivo control sobre la aplicación y su sistema permitirán garantizar una mayor salvaguardia de la seguridad y la protección de los datos de carácter personal, y de toda la información, tratados en *H&TeHealth*.

Sin embargo, no por ello debe olvidarse el derecho de acceso a la Historia Clínica de todo usuario paciente.

Se recomienda tomar todas las cautelas posibles para verificar que quien solicita el acceso es el verdadero interesado titular de los datos, y no un tercero no autorizado, pero sin entorpecer el ejercicio del citado derecho (véase **apartado 5.5** del informe).

[89] Marrero Pérez, M. (2011). Implicaciones Éticas Asociadas al Uso de la Telemedicina. *Revista eSalud*, Vol. 7, nº28.

[90] El peligro asociado a la Historia Clínica no es nuevo: en 1997, el Tribunal Supremo confirmó la condena al Instituto Nacional de la Salud por responsabilidad extracontractual del Hospital de La Princesa de Madrid por los daños y perjuicios sufridos por una persona física como consecuencia de la falta de guarda y custodia de su historia clínica. Hubo terceras personas no autorizadas que accedieron a aquélla y pudieron conocer que el paciente padecía de Sida, chantajeándole posteriormente por este hecho – Sentencia del Tribunal Supremo 452/1997, de 27 de enero de 1997.

[91] Aleixandre Benavent, R., Ferrer Sapena, A. y Peset Mancebo, M. F. (2010). Informatización de la historia clínica en España. *El profesional de la información*, Vol. 19, nº3 (pp. 231-239). Recuperado de: https://bit.ly/2Nk8OA5.

En este sentido, la revisión periódica de las medidas y procedimientos que a continuación se expondrán, con el fin de evaluar su adecuación en cada momento y en cada entorno, será de vital importancia a efectos de cumplir con la responsabilidad proactiva del Responsable del tratamiento con respecto de los datos que trata, así como para detectar posibles puntos débiles en el sistema o situaciones en que no se estén observando los derechos y libertades de los interesados.

6.3. Medidas de seguridad

A continuación se proponen una serie de medidas de seguridad de tipo técnico y organizativo en relación con el tratamiento de información y datos de carácter personal en el sistema de H&T.

El objetivo es que las medidas aquí recogidas, una vez implementadas, sirvan como demostración de cumplimiento de las obligaciones que el RGPD impone a los Responsables del tratamiento en términos de responsabilidad proactiva y privacidad desde el diseño. Recordemos que, en lo que respecta al objeto del presente informe, *H&T Hospitales* sería Responsable del tratamiento de aquellos datos tratados a través de la aplicación.

6.3.1. Medidas organizativas

Con el fin de gestionar la implementación de medidas de seguridad en la organización, es habitual encomendar las tareas de revisión, verificación y control de cumplimiento a un **Responsable de Seguridad**[92] que se encargue de supervisar que las medidas se adaptan a la normativa en materia de protección de datos y seguridad de la información, velando asimismo por el cumplimiento de aquéllas. No obstante, el principio de responsabilidad proactiva del RGPD traslada la decisión de nombrar uno al Responsable del tratamiento, sin que la norma establezca una obligación al respecto: su designación es facultativa.

En el caso de H&T, por el tratamiento de datos sensibles relativos a la salud y, en general, el tratamiento de información a gran escala, la figura del Responsable de Seguridad resulta recomendable a efectos de organización, unificando funciones en esta materia y

[92] Cortés Saavedra, J. M. (2017). El proceso de "compliance" y el responsable de seguridad. *Seguritecnia*, Nº442, pp. 106-110. Recuperado de: https://bit.ly/3hLnRAu.

contando con un factor impulsor del cumplimiento normativo en *H&T Hospitales* en este sentido.

6.3.1.1. Gestión de Personal

En el proceso de contratación de personal, el establecimiento de procedimientos por los cuales se firmen anexos a los contratos en relación con la protección de datos y la seguridad de la información, informando sobre los tratamientos de forma transparente, permite generar cultura de seguridad y privacidad de la información en una organización partiendo de su propio personal. Asimismo, la normativa interna en las organizaciones permite establecer un sistema paralelo con obligaciones y consecuencias de su incumplimiento, que dará lugar a responsabilidad disciplinaria[93], un aspecto punitivo que refuerza el papel proactivo del Responsable y el papel propio de la normativa interna.

Se recomienda elaborar anexos a los contratos de trabajo y colaboración con información sobre el tratamiento de datos de titularidad de los empleados, trabajadores autónomos, colaboradores, etc., que prevean, al menos, un compromiso básico de confidencialidad.

Asimismo, se recomienda elaborar un **Manual de Funciones y Obligaciones del Personal** para clarificar la estructura operacional y el correcto desenvolvimiento del personal en el marco de una cultura interna de seguridad de la información y privacidad.

Se recomienda también solicitar al personal la verificación periódica de sus datos mediante el Modelo 145 de la Agencia Tributaria, al menos anualmente.

En cuanto al **alta en los sistemas**, es preciso controlar que cada usuario tenga asignados los permisos de acceso y utilización de la información y datos de aquéllos en función de las necesidades de su puesto de trabajo o actividad en la organización, de forma que no se pueda acceder a recursos no necesarios.

Se recomienda implementar funcionalidades dirigidas a que los responsables correspondientes en H&T tengan la facultad de crear perfiles y usuarios con diversos

[93] La Sala de lo Social del Tribunal Superior de Justicia de Castilla-La Mancha confirmó una sentencia de primera instancia por la que se desestimaba la demanda por despido disciplinario de dos trabajadores de *Securitas Direct* que, incumpliendo el Código de Conducta de la compañía, utilizaron indebidamente información confidencial, en una clara transgresión de la buena fe contractual – Sentencia del Tribunal Superior de Justicia de Castilla-La Mancha (Sala de lo Social), de 9 de febrero de 2017 (Nº de Recurso 1697/2017). Disponible en: https://bit.ly/3hNCZxi.

niveles de acceso a la información, figurando todos ellos en un registro de usuarios en el que conste, al menos, el nombre, apellidos, perfil asignado y los permisos concedidos en el sistema.

Con respecto de los **usuarios del sistema y de la aplicación**, se recomienda lo siguiente:

Habilitar mecanismos para que los responsables puedan cerciorarse de que los usuarios no pueden modificar los roles y privilegios que les han sido asignados.

Asimismo, a efectos de autenticación, se recomienda implementar un **sistema de claves** para la correcta identificación del usuario en cuestión; y una **política de contraseñas** adecuada (cambio de clave tras el primer acceso, número mínimo de caracteres que incluya, símbolos, elementos alfanuméricos, mayúsculas y minúsculas; y un sistema de caducidad de claves que obligue a los usuarios a modificarlas, al menos, anualmente).

El acceso a recursos a los que habitualmente no se tiene acceso habrá de requerir, en todo caso, una solicitud motivada al Responsable de Seguridad, que valorará la necesidad del acceso y podrá proporcionar uno temporal a la información.

Desde la perspectiva de los facultativos de la unidad de oncología de H&T, es preciso que cada usuario únicamente tenga acceso a aquella información que necesite para desempeñar sus funciones, no pudiendo acceder a información que no deba.

En este sentido, un usuario administrador de H&T debería poder acceder al historial y datos completos de todos los usuarios, mientras que los demás usuarios únicamente deberían poder acceder y conocer los datos relevantes para su función dentro del equipo. En este sentido, la aplicación deberá permitir crear distintos usuarios en función de los perfiles de cada uno, y el Responsable, H&T, deberá llevar una relación actualizada de usuarios y perfiles con los accesos y permisos a que cada uno esté autorizado.

Se recomienda la creación de un usuario administrador correspondiente, por ejemplo, al jefe de la unidad de oncología de H&T, que tenga acceso a todos los historiales y datos de todos los usuarios, de forma que los usuarios correspondientes al resto del equipo médico sólo tengan acceso a aquellos datos que necesiten en función de sus respectivas actividades, como los datos de los pacientes en concreto que cada facultativo atienda en la teleconsulta o con los que se comunique a través de la aplicación.

En relación con la **baja de los sistemas**, se recomienda lo siguiente:

Que los permisos de acceso sean revocados de forma inmediata una vez ha desaparecido la necesidad que los motiva (en el caso de accesos temporales), o en casos de bajas de personal con privilegios de acceso.

6.3.1.2. Tratamiento de información fuera de las instalaciones de H&T Hospitales

En este punto se recomienda, con carácter general, que los datos procesados a través de *H&TeHealth*, en tanto en cuanto revestirán un carácter sensible en la mayoría de las ocasiones, no sean tratados fuera de las instalaciones de H&T.

Si concurriera alguna circunstancia que hiciera necesario este tratamiento, se habrán de tomar medidas para registrar la asignación de esta clase de permisos a los usuarios que así puedan llevarlo a cabo. En todo caso, deberá ser el Responsable de Seguridad el que autorizará este hecho y el que controlará qué dispositivos serán asignados a estos usuarios con el fin de que puedan conectarse al sistema de H&T desde fuera de sus instalaciones.

Algunas medidas de seguridad que se recomienda implementar en este supuesto serían, por ejemplo, la de la protección de los documentos o archivos mediante contraseña, la eliminación de aquéllos tras su envío con la llevanza de un registro de borrados, la prohibición del uso de soportes portátiles o similares para almacenar información, o la prohibición general de conexión remota que no se realice mediante VPN[94].

6.3.1.3. Incidencias y violaciones de seguridad

Los artículos 33 y 34 del RGPD determinan que, ante una brecha de seguridad en un sistema de información que comporte la pérdida o puesta en compromiso de información de índole sanitaria de los usuarios, se notifique este hecho a la AEPD en el plazo improrrogable de 72 horas tras la detección de la brecha, y que se informe igualmente a los interesados de tal hecho.

En el caso de una brecha de seguridad en *H&TeHealth*, debemos entender que la severidad de las consecuencias de aquélla para las personas físicas puede ser alta, debido a que podríamos encontrarnos con la pérdida de información sensible relativa a la salud

[94] Una VPN (*Virtual Private Network* / Red Virtual Privada) permite el acceso a recursos corporativos mediante la tecnología de red, conectando dispositivos a redes privadas a través de Internet.

de los usuarios (informes, radiografías, fotografías, Historia Clínica electrónica, etc.), lo que en el peor de los casos podría derivar indirectamente en el empeoramiento de la salud del paciente en función de su estado previo a la brecha y el tratamiento específico que se le estuviera administrando[95].

Se recomienda implantar un protocolo por el que se notifique cualquier incidencia al Responsable de Seguridad, que deberá registrar las incidencias haciendo constar su tipología, el momento en que se ha producido o detectado, la persona que la ha notificado, los efectos derivados de la incidencia y las medidas correctoras aplicadas para solventarla.

Asimismo, se recomienda que el Manual de Funciones y Obligaciones del Personal antes citado, recoja cuestiones relativas a los conceptos de incidencia y violación de seguridad, y las maneras de proceder ante ellas, con el contacto con el Responsable, el registro, y, si procede, la comunicación a la AEPD en el plazo establecido en casos de brechas de seguridad.

Habida cuenta de lo anterior, se recomienda la elaboración de una **política de notificaciones de brechas de seguridad**.

6.3.1.4. Gestión de soportes

El **etiquetado** de soportes y documentos de manera que los usuarios con acceso a aquéllos puedan conocer el tipo de contenido que comprenden afianza aún más la seguridad y el control de accesos a la información.

Se recomienda que el Responsable de Seguridad defina la metodología de archivo de la información de forma tal que, junto al etiquetado, los usuarios autorizados puedan localizarla y consultarla rápidamente, lo que a la postre facilitará el ejercicio de los derechos de protección de datos por parte de los interesados.

En cuanto a la **destrucción de soportes y borrado de la información**, se recomienda lo siguiente:

Que se lleve a cabo un **inventario de activos** de la organización (para el seguimiento de dispositivos y personas responsables de los mismos mediante, por ejemplo, un etiquetado

[95] AEPD. (2018). *Guía para la gestión y notificación de brechas de seguridad*. Recuperado de: https://bit.ly/2BkFQ01.

mediante código QR[96] que permita la identificación del dispositivo de forma unívoca) y, en la medida de lo posible, organizar la **destrucción certificada** de soportes e información por medio de empresas externas que garanticen la validez del proceso de destrucción y acorde con la normativa.

En el caso de soportes informáticos, se recomiendan medidas como el formateo y la comprobación del efectivo borrado de la información; mientras que en el caso de soportes físicos se recomienda la utilización de destructoras. Asimismo, la desmagnetización, destrucción y sobreescritura son medidas igualmente útiles en el campo de la información almacenada en soportes informáticos.

En este punto, debe traerse a colación el plazo de conservación legal al que determinados datos deben estar sujetos. En el caso de la documentación clínica, como se ha puesto de manifiesto en el presente informe, existe una obligación legal de conservación de, al menos, cinco años desde la fecha de alta de cada proceso asistencial.

Se recomienda implantar una **política de supresión y bloqueo de información** que prevea los diversos plazos de conservación a los que se enfrentará cada dato en función de su naturaleza y tipología (véase **apartado 5.4.3** del presente informe).

6.3.2. Medidas técnicas

6.3.2.1. Copias de seguridad

Las copias de seguridad se conforman como el proceso por el que se duplica información de un soporte a otro, con el objetivo de que tal información pueda ser recuperada en el supuesto en que el alojamiento de los datos del primer soporte presente alguna clase de fallo o error. En el caso de *H&TeHealth*, la información tratada mediante la aplicación es la piedra angular del servicio, de forma que la pérdida de tal información supondría graves consecuencias no sólo para la continuidad del modelo de servicio de telemedicina analizado, sino también desde la perspectiva de la privacidad y la salud de las personas.

De este modo, las copias de seguridad cumplen una doble función: por un lado, permiten evitar que se destruya o pierda información relevante de manera definitiva; y por otro lado, de cara a un eventual ataque malintencionado al sistema de información, permite

[96] Un código QR (*Quick Response* / Respuesta Rápida) es un código de barras bidimensional de forma cuadrada que permite almacenar datos de manera codificada.

habilitar múltiples líneas de defensa para ganar tiempo, minimizar el impacto y reducir el compromiso global de un sistema de información.

Los criterios a los que debe responder la clasificación de la información a efectos de relacionarlos con las medidas de seguridad aplicadas y con los mecanismos de copias de seguridad son los siguientes: nivel de accesibilidad o confidencialidad, utilidad o funcionalidad, e impacto en caso de pérdida de la información por cualquier causa[97].

En cuanto a la periodicidad con la que se deberán realizar las copias de seguridad, se ha de tener en cuenta el número de archivos generados, el coste de almacenamiento, y las obligaciones legales derivadas de normas como el RGPD. Valorando estas cuestiones en conjunto se podrá determinar el tipo de copia de seguridad más adecuada para la organización[98].

En relación con los soportes de las copias de seguridad, existen múltiples soluciones más o menos recomendables en función del tamaño de la organización: cintas magnéticas, discos duros HDD y SDD, dispositivos NAS[99], la nube, etc. En el caso de la nube se debe tener en cuenta que las organizaciones prestadoras de servicios de almacenamiento en la nube presenten las garantías de seguridad necesarias en términos de respaldo y recuperación de la información. De igual manera, las soluciones C2C (*Cloud to Cloud*) en las que las copias de seguridad se realizan desde un software en la nube, como aplicaciones, a un servicio de copias en la nube.

Se recomienda seguir una **estrategia de copias de seguridad en "3-2-1"**, tal y como recomienda el INCIBE-CERT: mantener tres copias de cualquier información considerada importante (la original y dos copias de seguridad); almacenar las copias en dos soportes distintos, para reducir el nivel de compromiso en términos de soportes; y

[97] INCIBE-CERT. (2018). *Copias de seguridad: una guía de aproximación para el empresario*. Recuperado de: https://bit.ly/3fIDWoP.

[98] A grandes rasgos, existen cuatro clases de copia de seguridad: (1) **Copia de seguridad en espejo**, consistente en la copia exacta y en tiempo real de la información mientras se trabaja sobre la misma; (2) **Copia de seguridad completa**, consistente en la copia de todos los datos del sistema en un segundo soporte; (3) **Copia de seguridad diferencial**, consistente en la sola copia de todos aquellos datos creados y modificados desde la copia completa anterior; y (4) **Copia de seguridad incremental**, consistente en la copia de los datos creados y modificados desde la última copia realizada, completa o diferencial, comparando fechas de modificación de los datos y copiando aquellos de fecha más reciente – Crocetti, P. (24 de julio de 2019). Tipos de copias de seguridad explicados: incremental, diferencial o de espejo. *SearchDataCenter*. Recuperado de: https://bit.ly/2YYJ1mp.

[99] Un dispositivo NAS (*Network Attached Storage* / Almacenamiento Conectado en Red) permite el almacenaje y la recuperación de datos en un punto centralizado para todos los usuarios autorizados en el sistema, mediante la conexión a la red.

almacenar una copia de seguridad fuera de las instalaciones de *H&T Hospitales* (por ejemplo, en un servicio externo de almacenamiento en la nube).

Se recomienda, asimismo, contar con **copias completas a partir de las que puedan realizarse copias incrementales** en función de los archivos creados y modificados, siendo esta la solución óptima en términos de espacio de almacenamiento, tiempo de realización de las copias y recuperabilidad de los datos. Aunque las copias en espejo pueden resultar atractivas, debe tenerse en cuenta que en supuestos como el borrado accidental de un archivo conllevará su borrado también en la copia de seguridad.

En términos de soportes, habida cuenta del tamaño de la Unidad de Oncología de H&T en Madrid, se recomienda el uso de un **dispositivo NAS** a nivel interno con el añadido de un servicio externo de **almacenamiento en la nube**, sin perjuicio de la existencia de soportes adicionales como discos duros.

Finalmente, en cuanto a la periodicidad, se recomienda la realización de copias de seguridad, al menos, **semanales**. Así, podría establecerse una política de realización de **copias completas mensuales y copias incrementales al finalizar cada semana**, de forma que siempre exista una copia de seguridad actualizada de toda la información en H&T, con la consecuente llevanza de un registro de copias por parte del Responsable de Seguridad.

La protección de las copias de seguridad mediante cifrado, contraseñas y la verificación de las copias deberá formar parte integrante de las políticas y estrategias de copias de seguridad en H&T.

6.3.2.2. Cifrado

La criptografía viene utilizándose paralelamente al desarrollo del propio lenguaje escrito como técnica de protección de comunicaciones frente a intercepciones ajenas no autorizadas[100]. De esta manera, la criptografía se utiliza para proteger cualquier clase de comunicación de datos, desde transacciones financieras hasta comunicaciones de datos altamente confidenciales como los relativos a la salud[101], en lo que interesa desde la perspectiva del presente informe, ya que permite garantizar la privacidad y la

[100] Singh, S. (2000). *Los códigos secretos*. Madrid: Debate.
[101] Koomen, M. (2019). The Encryption Debate in the European Union. *Carnegie Endowment for International Peace*. Recuperado de: https://bit.ly/2Zrcl5h.

inviolabilidad de las comunicaciones en cualquier sistema de almacenamiento, procesamiento y transmisión de información.

Las técnicas criptográficas forman parte de un conjunto de medidas técnicas de seguridad que, sumadas a las organizativas, a las copias de respaldo y controles de accesos al sistema, permiten incrementar la garantía de confidencialidad e integridad de la información. Asimismo, las firmas digitales que facilita la criptografía permiten también garantizar la autenticidad y no repudio de la información[102].

El cifrado presenta, por tanto, tres funciones básicas que se despliegan en tres de los aspectos relevantes de la seguridad de la información: la confidencialidad de esta, su disponibilidad y su integridad[103]. El objetivo de esta medida es aumentar la protección de la información, fortaleciendo la seguridad de soportes y contenidos y dificultando la posibilidad de fugas.

Aunque existen múltiples métodos de cifrado (cifrado César, cifrado de Vigenère, Entropía, etc.)[104], este consiste, básicamente, en la conversión de datos en conjuntos de letras, símbolos o números que sólo pueden conocerse si se conoce la clave que permite descodificar aquello que se ha cifrado. En este sentido, el sistema de cifrado podrá ser simétrico o asimétrico, según exista una sola clave privada o la conjunción de una privada y una pública.

Se recomienda elaborar un **inventario de activos y recursos que se protegerán por cifrado**, atendiendo a criterios como su sensibilidad o nivel de confidencialidad, tal y como se ha indicado en el apartado relativo a las copias de seguridad. Por ejemplo, es aconsejable encriptar los discos duros externos y demás soportes de información, dotando de mayor seguridad y niveles más altos de protección a la información contenida en los mismos.

[102] INCIBE-CERT. (2018). *Uso de técnicas criptográficas*. Recuperado de: https://bit.ly/2V456hU.
[103] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, de 8 de octubre de 1997, sobre el fomento de la seguridad y la confianza en la comunicación electrónica – Hacia un marco europeo para la firma digital y el cifrado (COM 97/503). Recuperado de: https://bit.ly/312wHUv.
[104] Gómez, S.; Arias, J.D. y Agudelo, D. (2012). Cripto-análisis sobre métodos clásicos de cifrado. *Scientia et Technica*, Vol. 2 (nº50), pp. 97-102.

En definitiva, el cifrado aporta ventajas en relación con el establecimiento de múltiples niveles de seguridad en un sistema, la obtención de una administración centralizada y el cumplimiento de unos estándares de seguridad de alto nivel.

Se recomienda utilizar el método de cifrado más potente posible, con claves extensas y seguras. Asimismo, se recomienda no almacenar las claves junto a los datos encriptados. Si bien parece una recomendación lógica, no son pocas las ocasiones en que se dan accesos no autorizados a información protegida por no haber dotado a las claves de la seguridad debida.

6.3.2.3. Actualización y bloqueo de dispositivos

Es preciso que el Responsable de Seguridad vele por que los diversos dispositivos que se utilicen en relación con *H&TeHealth* se encuentren actualizados en todo momento, con especial atención a los programas antivirus, *firewalls* o cualquier otro tipo de software que pueda ser objeto de brechas de seguridad por haber quedado desfasado.

Se recomienda implantar una **política de actualización periódica**, de periodicidad mensual, por la que los usuarios deban comprobar el estado de las actualizaciones de sus correspondientes equipos y dispositivos con acceso a los sistemas de información y, en su caso, proceder a instalar las actualizaciones pertinentes.

En este sentido, cabe recomendar que el Responsable de Seguridad desempeñe un papel activo por el que verifique la concurrencia de nuevas actualizaciones y se encargue de informar de ello a la plantilla por medio de circulares, con el fin de que la instalación de actualizaciones no deba esperar necesariamente al siguiente momento de comprobación mensual establecido en la política de actualización periódica.

En lo que respecta al bloqueo de dispositivos, se trata de una medida esencial para la preservación de la confidencialidad, integridad y disponibilidad de la información, tan básica como el establecimiento de un sistema de contraseñas. De este modo, aquellos equipos y dispositivos que se encuentren inactivos durante un determinado período de tiempo deberán quedar bloqueados (su fijación dependerá del Responsable de Seguridad). Así, ante un acceso a la información contenida en el dispositivo bloqueado se deberá introducir un usuario y contraseña, evitando posibles figas de información y reforzando la seguridad de la información.

Se recomienda que los dispositivos queden bloqueados tras un lapso de tiempo de inactividad lo más corto posible, sin que ello acabe resultando tedioso para el usuario autorizado -cinco minutos, por ejemplo-.

Esta cuestión debe ser tratada en el Manual de Funciones y Obligaciones del Personal, a efectos de que los diversos usuarios adquieran la obligación de fijar el usuario y la contraseña específicos en los dispositivos de su responsabilidad.

7. Análisis de riesgos final

La aplicación de todas las medidas recomendadas en el presente informe, en términos de privacidad desde el diseño y por defecto, por un lado, y de seguridad de la información, por otro, debiera dar lugar a la disminución del riesgo en los tratamientos de *H&TeHealth*. En virtud de la adopción de tales medidas, devendrá necesario realizar un último análisis de riesgos de cuyo resultado dependerá la necesidad de realizar, o no, una Evaluación de Impacto en la Protección de Datos.

El artículo 35 del RGPD establece que cuando sea probable que un tratamiento, "*por su naturaleza, alcance, contexto o fines*", entrañe un alto riesgo para los derechos y libertades de las personas físicas, el Responsable del tratamiento deberá realizar una EIPD de tales operaciones de tratamiento. El precepto, de hecho, matiza específicamente que la utilización de nuevas tecnologías puede suponer un probable alto riesgo para tales derechos y libertades. La elaboración de perfiles, asimismo, figura como uno de los casos en que la EIPD será necesaria, en el apartado 3 del artículo 35.

Así, los tratamientos que impliquen el perfilado de interesados, con la recogida de datos relativos no sólo a la salud sino a diversos ámbitos de la vida de aquellos sobre sus hábitos; los tratamientos que impliquen el uso de categorías especiales de datos del artículo 9.1 del RGPD (datos relativos a la salud); y los tratamientos que impliquen la utilización de nuevas tecnologías; requieren una EIPD por entrañar un alto riesgo para los derechos y libertades de los interesados, tal y como posteriormente a la entrada en vigor del RGPD han señalado tanto la AEPD[105] como el GT29[106] (hoy CEPD). Ante un alto riesgo persistente, la EIPD entraría en juego en estos casos.

Pues bien, en el caso de *H&TeHealth* el análisis de riesgo inicial había volcado una serie de amenazas propias del Chatbot, por un lado (decisiones equivocadas o discriminatorias); y amenazas propias del sistema de información de la aplicación (accesos no autorizados a la información, brechas de seguridad, etc.). Las medidas recomendadas en este informe, debidamente aplicadas, permiten rebajar los riesgos

+[105] AEPD. (2019). *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*. Recuperado de: https://bit.ly/2MYCLVQ.
[106] GT29. (4 de abril de 2017). *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679* (WP 248). Recuperado de: https://bit.ly/2ULWmgC.

detectados a un mínimo tolerable en términos de protección de datos y seguridad de la información.

Con respecto del Chatbot, se han delimitado sus finalidades y se han minimizado los datos, con la posterior anonimización de estos para fines estadísticos, reduciendo la personalidad de los datos y eliminando la posibilidad de asociarlos a personas identificadas o identificables. Con respecto de la aplicación en sí, se han implementado medidas técnicas y organizativas dirigidas a informar debidamente a los interesados, facilitar el ejercicio de derechos por su parte y asegurar la confidencialidad, la integridad, la autenticidad, la disponibilidad y la trazabilidad de sus datos y de la información almacenada y procesada en el sistema de H&T, con el fin de minimizar todo lo posible el impacto producido por eventuales supuestos indeseados como pérdidas de información, brechas de seguridad, accesos no autorizados, etc.

De este modo, cabe concluir que se han recomendado e implementado medidas diseñadas desde un enfoque de riesgos, como recomienda la AEPD a tal efecto[107], de forma que se posibilita una adecuada gestión de los riesgos existentes en el ciclo de vida de los datos asociados a todos los tratamientos que con *H&TeHealth* se estarán llevando a cabo.

En este punto resultan de especial interés los esquemas de certificación, tales como los de las normas ISO/IEC[108]. La norma ISO/IEC 29100[109] permite definir medidas de salvaguardia de la privacidad mediante una terminología común, la definición de los roles de las partes implicadas en el procesamiento de datos, los requerimientos de seguridad y la referencia a principios de privacidad como la legitimación y la minimización.

[107] AEPD. (25 de mayo de 2018). *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD*. Recuperado de: https://bit.ly/37xbCCS.

[108] La ISO (*Internacional Organization for Standardization*) e la IEC (*Internacional Electrotechnical Commission*) son dos organizaciones de normalización y estandarización que desde hace años emiten normas o estándares de aseguramiento de la calidad, la seguridad y la eficiencia de determinados productos, servicios y sectores de la economía. Individualmente, emiten sus respectivas Normas ISO y Normas IEC, pero conjuntamente emiten normas ISO/IEC, de mayor alcance geográfico y combinando entornos de múltiples partes interesadas. El paradigma de este tipo de normas conjuntas es la serie ISO/IEC 20000, el estándar internacionalmente reconocido en el marco de la gestión de servicios TIC.

[109] Norma Internacional ISO/IEC 29100 (2011). *Tecnología de la Información – Técnicas de seguridad – Marco de privacidad*. Suiza: ISO. Recuperado de: https://bit.ly/3fxjNlx.

8. Conclusiones

La realización del presente informe se ha basado en las consideraciones y recomendaciones más garantistas a la luz de la legislación y jurisprudencia vigentes en materia de sociedad de la información y comercio electrónico, protección de datos y seguridad de la información, así como con base en la información facilitada por *H&T Hospitales* hasta la fecha de su realización. No obstante, el presente informe queda sujeto a mejor opinión fundada en Derecho y a la legislación y demás jurisprudencia que pueda devenir vigente a partir de ahora.

Las siguientes conclusiones pretenden recoger, a grandes rasgos, las cuestiones que han sido tratadas a lo largo del informe, como epílogo y resumen de este.

Aun a pesar del entorno digital en el que se desenvolverá *H&TeHealth*, con la novedad que la aplicación en sí implica en cuanto a la prestación del servicio de consultas médicas, no debe perderse de vista que las teleconsultas, como parte de la telemedicina, cumplen los requisitos para ser consideradas como servicio sanitario, lo cual las sujeta a un régimen regulatorio específico en términos de autonomía del paciente y a unos principios propios del sector de la salud. De este modo, el aseguramiento de la identidad de las partes y la información previa al usuario paciente en aras de obtener su consentimiento informado para proceder a una teleconsulta se conforman como los dos pilares fundamentales sobre los que la prestación del servicio debe sustentarse y sobre las que la aplicación debe partir.

Asimismo, las características de *H&TeHealth*, de sus servicios y funcionalidades, hacen que debamos encajarla en el concepto de servicio de la sociedad de la información, y a *H&T Hospitales* como prestador de servicios de la sociedad de la información en lo que respecta a la aplicación, lo que supone la aplicación de la normativa de Internet. Esto suma una serie de obligaciones adicionales de cara a los usuarios en el tráfico digital, como la información general sobre el titular que se encuentra detrás de *H&TeHealth*, sobre las condiciones de uso de la aplicación y sobre la utilización de tecnologías como las cookies. Asimismo, la posibilidad de contratar el servicio de teleconsultas a través de la aplicación hace que se deba facilitar un marco transparente de contratación electrónica respetando, a su vez, la legislación en materia de defensa de consumidores y usuarios.

Para la prestación de tales servicios de teleconsultas y el desenvolvimiento de las funcionalidades de la aplicación, como el Chatbot, se requerirá el tratamiento de datos de

carácter personal de los usuarios de aquélla. La piedra angular, en este sentido, se encuentra localizada en los datos relativos a la salud, ya que serán estos los principales activos a la hora de la correcta prestación del servicio en la aplicación. La concurrencia de datos y la sensibilidad de estos últimos hará necesario que el tratamiento de aquéllos realizado a través de *H&TeHealth* se amolde a los principios del tratamiento recogidos en el RGPD, limitando finalidades y minimizando los datos en la medida de lo posible. El análisis de riesgos inicial, que evalúa el nivel de riesgo existente en relación con la aplicación, ha resultado en un alto riesgo para los derechos y libertades de los interesados, habida cuenta de la concurrencia de datos sensibles relativos a la salud, el uso de herramientas tecnológicas y el tratamiento a gran escala que se dará a través de *H&TeHealth*, lo que inevitablemente lleva a la necesidad de implementar medidas de seguridad y privacidad desde el diseño que permitan reducir el riesgo a un mínimo tolerable.

Entre tales medidas podemos encontrar algunas relativas a la correcta identificación y autenticación de usuarios en la aplicación, para evitar accesos no autorizados, mediante mecanismos de doble validación; la prestación de toda la información requerida en virtud de la normativa en forma de avisos y políticas de privacidad fácilmente accesibles y comprensibles para los usuarios; y la supresión y el bloqueo de información cuanto esta deviene innecesaria, en función de la naturaleza de cada tratamiento y de sus respectivas bases de legitimación. El ejercicio de derechos por parte de los interesados, asimismo, se presenta como uno de los puntos fuertes de la política a implantar. También se añaden medidas organizativas tales como la diligente y documentada elección de proveedores externos que vayan a tratar datos por cuenta de H&T en el marco de sus actividades, y la designación de un Delegado de Protección de Datos, que en este caso resulta preceptiva, para reforzar la gestión adecuada de todo lo relacionado con los tratamientos y la protección de datos en la organización.

El resto de las medidas recomendadas, tanto organizativas como técnicas, abordan la seguridad de la información como eje fundamental en *H&TeHealth*, y H&T en sí, desde un enfoque de riesgos. En aras de garantizar la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información es necesario que, una vez identificados los activos y los riesgos del sistema de información de la aplicación, se proceda a implementar medidas de gestión de personal y de soportes, así como de gestión de perfiles y permisos de acceso al sistema de información, y de las incidencias de seguridad que

eventualmente puedan concurrir en aquél. Asimismo, desde una visión más técnica, las copias de seguridad y el cifrado se conforman, junto a la actualización y bloqueo de dispositivos, como las principales medidas a adoptar en esta materia.

De este modo, el análisis de riesgos final ha constatado que, aplicando todas y cada una de las medidas técnicas y organizativas recomendadas, los riesgos asociados a los tratamientos de datos e información en H&TeHealth se podrán reducir a un mínimo tolerable a la luz de la normativa, lo que a la postre implica la no necesidad de realizar una EIPD.

ANEXOS

Anexo I: Aviso Legal

H&T Hospitales, S.A., (en adelante el Titular o H&T), con NIF A12345678 y domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid), e inscrita en el Registro Mercantil de Madrid, Tomo: 12345, Folio: 12, Sección: 123, Hoja Registral: M-12345, Inscripción: 1, es titular de la aplicación accesible a través de la URL: https://es.h&tehealth.com/ (en adelante, *H&TeHealth*).

Si tienes alguna consulta, duda o sugerencia que desees realizar con respecto de *H&TeHealth*, puedes contactar con nosotros en la dirección de correo electrónico hola@h&tehealth.com, o en el número de teléfono 912 34 56 78.

A continuación procedemos a mostrarte las condiciones que regulan el acceso a nuestra aplicación, sus servicios y sus funcionalidades. Te recomendamos que revises este texto de forma periódica.

Nuestros facultativos

El equipo de H&T está formado por médicos especialistas con amplia experiencia en el campo de la oncología. A continuación te detallamos los datos de nuestros profesionales:

D. Jorge Ortiz Díaz

Colegio de adscripción: Ilustre Colegio Oficial de Médicos de Madrid

Nº de Colegiado: 12345678

Miembro de la Sociedad Española de Oncología Médica

Dña. Daniela Benítez Pérez

Colegio de adscripción: Ilustre Colegio Oficial de Médicos de Madrid

Nº de Colegiado: 23456789

Miembro de la Sociedad Española de Oncología Médica

Dña. Estíbaliz Cortés Alcázar

Colegio de adscripción: Ilustre Colegio Oficial de Médicos de Madrid

Nº de Colegiado: 34567890

Condiciones Generales de Uso

1. Identificación de las partes

Las presentes Condiciones se suscriben por nosotros, el Titular, y por ti, como Usuario que accede voluntaria, libre y gratuitamente a nuestra aplicación, y se aplicarán con independencia de que se proceda, o no, a la contratación de nuestro servicio de teleconsulta de *H&TeHealth*.

2. Objeto de *H&TeHealth*

La aplicación tiene como objeto la prestación de un servicio de teleconsulta y una funcionalidad de Chatbot, así como informar sobre nuestros servicios y funcionalidades. El acceso y la navegación por la aplicación son gratuitos, aunque la contratación de nuestro servicio de teleconsulta conlleva el abono de un precio y la aceptación de nuestras Condiciones Generales de Contratación[110].

3. Obligaciones del Usuario

Como Usuario, cuando accedes y navegas por *H&TeHealth*, debes:

a. Usar la aplicación de forma diligente, correcta y lícita, respetando la legislación vigente, la moral y el orden público, así como las buenas costumbres.
b. Revisar de forma regular estas Condiciones, así como cualesquiera otras aplicables, para comprobar las modificaciones que pudieran haberse producido.
c. Revisar las comunicaciones que te remitamos, pueden contener información importante sobre la aplicación.
d. No usar la aplicación con fines comerciales, ni que atenten contra la competencia con respecto de H&T Hospitales, S.A.
e. No modificar la aplicación, ni simular su apariencia o funcionalidades.
f. No dañar, deshabilitar, sobrecargar o dificultar el servicio, ni interferir en su uso y disfrute.
g. No introducir virus informáticos o cualesquiera otros códigos maliciosos ideados para interrumpir, destruir o limitar las funcionalidades de la aplicación.
h. No emplear técnicas de ingeniería inversa con el fin de revelar el código fuente de la aplicación.
i. No realizar actos que puedan vulnerar nuestros derechos e/o intereses, o de terceros, como los derechos de propiedad intelectual e industrial.

4. Disponibilidad de la aplicación

Aunque tratamos de mejorar *H&TeHealth* constantemente, la aplicación se mostrará tal y como se encuentre en cada momento según su disponibilidad, limitaciones y demás circunstancias concurrentes en cada caso.

[110] Enlace a las Condiciones Generales de Contratación de la aplicación.

5. Condiciones Particulares de Registro

Las Condiciones Particulares de Registro se suscriben por nosotros, H&T Hospitales, S.A., y el Usuario que haya completado el formulario de registro y creación de cuenta, junto a la aceptación de estas condiciones.

5.1. Creación de cuenta

Para crear una cuenta en *H&TeHealth*, el Usuario deberá ser una persona física mayor de edad.

El Usuario deberá acceder a la opción "*Registro*", introducir los datos identificativos y de contacto solicitados, y crear una contraseña. Deberá completar los pasos que se irán indicando, entre los que se encuentra la lectura de la información relativa a la Política de Privacidad[111] y de las presentes Condiciones.

El registro será confirmado al Usuario mediante una comunicación de bienvenida en la que el Usuario deberá ratificar el registro, momento a partir del cual pasará a ser Usuario Registrado.

Si un Usuario Registrado olvida o pierde su contraseña, deberá hacer clic sobre el enlace "*He olvidado mi contraseña*", introducir la dirección de correo electrónico a través de la cual efectuó el registro y contestar a las preguntas de seguridad, para el restablecimiento de aquélla.

Nos reservamos el derecho de comprobar y verificar la identidad del Usuario Registrado en cualquier momento, ya que el no cumplimiento de los requisitos indicados o el engaño en cuanto a su identidad, nos facultará para dar de baja en cualquier momento a tal Usuario, eximiéndonos de cualquier tipo de responsabilidad.

5.2. *H&TeHealth*

Los Usuarios Registrados podrán acceder a la contratación del servicio de teleconsultas de la aplicación, así como proceder a interactuar con nuestro Chatbot.

5.3. Obligaciones del Usuario Registrado

El Usuario Registrado debe:

a. No registrarse con varias cuentas, ni proceder a ello con datos falsos o suplantando la identidad de terceras personas.
b. No utilizar la cuenta de otro Usuario Registrado sin su expresa autorización o consentimiento.
c. Ser el responsable único de todas las actividades realizadas desde su cuenta en *H&TeHealth*. Será responsable de cualquier daño o perjuicio sufrido por terceros

[111] Enlace a la Política de Privacidad de la aplicación.

como consecuencia del incumplimiento de las presentes Condiciones, y será responsable de todo aquello que suceda en su cuenta personal, salvo que su seguridad se vea comprometida por actuaciones o causas ajenas al Usuario Registrado.

d. Cuidar la confidencialidad de sus datos. En concreto, deberá:
    a. Mantener la cuenta actualizada.
    b. Almacenar la contraseña de manera confidencial.
    c. Ser el único Usuario que utilice la cuenta.
    d. No transferir la cuenta a terceros de modo alguno.
e. Nos reservamos el derecho de verificar el perfil del Usuario, con el fin de eliminar o suspender la cuenta personal en caso de incumplimiento de las presentes Condiciones o de cualesquiera otros aplicables.

5.4. Modificación y cancelación de la cuenta

En cualquier momento, el Usuario Registrado podrá modificar los datos de su cuenta personal en la aplicación. Asimismo, podrá cancelarla a través del área personal de usuario.

6. Exclusión de responsabilidad

H&T Hospitales, S.A., trabaja para que los servicios y funcionalidades de la aplicación se encuentren siempre disponibles. No obstante, cuando se acceda a ésta, la aplicación será mostrada según la disponibilidad y las limitaciones que concurran en cada caso.

H&T Hospitales, S.A., emplea los estándares de seguridad habituales en Internet para proteger los sistemas y contenidos incluidos en *H&TeHealth*. No obstante, no es posible ofrecer una garantía plena en cuanto a intrusiones o pérdidas de información que puedan producirse eventualmente. Tampoco puede garantizarse la ausencia de virus u otros elementos dañinos en la aplicación que puedan alterar el dispositivo del Usuario. Por ello, el Usuario asume y comprende que existen situaciones que pueden escapar al control de H&T Hospitales, S.A.

H&T Hospitales, S.A., no asume la responsabilidad sobre los sitios de terceros a los que lleven enlaces incluidos en *H&TeHealth*.

H&T Hospitales, S.A., queda eximida de cualquier responsabilidad derivada del mal uso de la aplicación por parte de los Usuarios, o del incumplimiento de las obligaciones asumidas por los Usuarios en virtud de estas condiciones o cualesquiera otras aplicables.

7. Derechos de propiedad intelectual e industrial

Los derechos de propiedad intelectual e industrial sobre *H&TeHealth* y sus contenidos (programación, diseño, gráficos, códigos, textos, imágenes, marcas, nombres comerciales, signos distintivos, etc.) pertenecen en exclusiva a H&T Hospitales, S.A. En caso contrario, H&T Hospitales, S.A., contará con derechos y/o autorizaciones bastantes para la explotación de tales elementos.

La reproducción, distribución, comunicación pública, transformación o cualquier otra forma de explotación, quedan prohibidas, salvo que se cuente con el consentimiento previo, expreso y por escrito de H&T Hospitales, S.A., o del titular de los derechos afectados.

Si detectas alguna infracción en relación con esta materia, te rogamos que nos lo comuniques en la dirección de correo electrónico indicada más arriba.

8. Indemnización

8.1. Podemos sancionar a los Usuarios que incumplan las condiciones aplicables con la imposibilidad de acceder a la aplicación, de forma temporal o indefinidamente, sin que el Usuario tenga derecho a indemnización alguna por esta causa. La duración de tal sanción dependerá de la infracción cometida.

8.2. Cualquier daño, perjuicio, pérdida o coste en que incurramos, derivado del incumplimiento de estas Condiciones o de cualesquiera otras que resultaren aplicables por parte del Usuario, deberá ser debidamente resarcido por el Usuario que lo causó.

9. Modificaciones

Las presentes Condiciones pueden ser modificadas y/o actualizadas en cualquier momento sin necesidad de previo aviso. Las modificaciones y/o actualizaciones entrarán en vigor desde el momento en que sean publicadas en la aplicación.

10. Otras cuestiones

10.1. Salvaguardia e interpretación

Si la Autoridad competente declarara ilegal, inválida o no ejecutable alguna de las disposiciones de estas Condiciones, tal disposición deberá pasar a ser interpretada de la manera más próxima a la intención original de aquélla. En cualquier caso, la declaración de la Autoridad competente con respecto de tal disposición o cláusula no perjudicará la validez de las demás.

10.2. Idioma

El idioma aplicable a nuestras Condiciones es el español. Si facilitamos versiones en otros idiomas será por cortesía y para mayor comodidad para los Usuarios, de forma que en caso de contradicción entre diferentes versiones idiomáticas, prevalecerá la versión en español.

10.3. Legislación y fuero

Las relaciones entre el Usuario y nosotros se regirán por la legislación española.

El fuero para la resolución de las eventuales controversias en torno a estas Condiciones dependerá de que el usuario ostente, o no, la condición de consumidor y/o usuario. Siendo consumidor y/o usuario, las controversias se someterán a los Juzgados y Tribunales del domicilio del Usuario. En caso contrario, las controversias se dirimirán en los Juzgados y Tribunales de la villa de Madrid.

Anexo II: Condiciones Generales de Contratación

1. Identificación de las Partes

Las presentes Condiciones Generales de Contratación regulan la contratación de nuestro servicio de teleconsultas de *H&TeHealth*. Las partes intervinientes en la contratación, son:

a. H&T Hospitales, S.A., (en adelante, H&T), con NIF A12345678 y domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid), inscrita en el Registro Mercantil de Madrid, Tomo: 12345, Folio: 12, Sección: 123, Hoja Registral: M-12345, Inscripción: 1, es titular de la aplicación *H&TeHealth* accesible a través de la URL: https://es.h&tehealth.com/ (en adelante, la aplicación).
b. "Usuario", como toda persona física mayor de edad registrada en la aplicación y que complete los pasos dirigidos a la contratación del servicio, libre y voluntariamente, incluyendo la aceptación de las presentes Condiciones Generales de Contratación.

Si tienes alguna consulta, duda o sugerencia que desees realizar con respecto de nuestro servicio, puedes contactar con nosotros en la dirección de correo electrónico hola@h&tehealth.com, o en el número de teléfono 912 34 56 78.

2. Objeto

El objeto de las presentes Condiciones es regular la contratación del servicio de teleconsultas ofertado en la aplicación, a cambio del precio indicado, previa aceptación de estas Condiciones.

3. Proceso de contratación

En la página de "*Teleconsultas*" de *H&TeHealth* el Usuario obtendrá información acerca del objetivo y la metodología de nuestros facultativos a la hora de atender a los Usuarios pacientes a través de nuestro sistema de teleconsultas. Desde ahí, podrá acceder directamente al proceso de contratación del servicio.

Alternativamente, si el Usuario ha interactuado previamente con nuestro Chatbot, el propio Chatbot, en función de las respuestas e informaciones obtenidas y procesadas, recomendará al facultativo con el que más conveniente sea fijar una consulta con base en su especialización y, en consecuencia, enlazará al Usuario con el sistema de contratación de teleconsultas.

A continuación, deberá:

a. Hacer clic sobre el botón "*Quiero una teleconsulta*".
b. A continuación aparecerá un menú en el que el Usuario podrá seleccionar al facultativo con el que desee fijar una consulta (fuera del supuesto de la interacción previa con el Chatbot). Si previamente se han contratado consultas con uno de

nuestros facultativos, el sistema le redirigirá a este en la selección, salvo cambios por parte de nuestro Equipo Médico.

c. Tras la selección del profesional, se mostrará un calendario en el que el Usuario podrá obtener la disponibilidad de sus consultas, entre las que el Usuario podrá seleccionar la que mejor se adapte a sus horarios.
d. Será necesario que el Usuario seleccione el método de pago escogido. Actualmente, los medios de pago disponibles son:
    a. Tarjeta de débito o crédito.
    b. PayPal.
e. Tras facilitar los datos, se dará la oportunidad al Usuario de revisar su solicitud y, tras ello, en función del método de pago seleccionado, podrá proceder al pago y, con ello, a la confirmación de su voluntad de contratar y formalizar la contratación de nuestro servicio de teleconsulta, previa aceptación de estas Condiciones.
f. Confirmaremos la recepción de la solicitud la solicitud y, en su caso, el pago del servicio mediante correo electrónico, que incluirá la correspondiente factura en formato electrónico.

4. Servicio

H&TeHealth permite a sus usuarios contratar un servicio de teleconsultas con los facultativos de nuestra unidad de oncología de H&T Hospitales, con la posibilidad de transmisión de información y documentación en tiempo real. Las teleconsultas son libremente fijadas por los Usuarios en función de la disponibilidad de nuestros profesionales, con elección igualmente libre de facultativo.

Existe la posibilidad, además, de interactuar previa y gratuitamente con nuestro Chatbot, que recopilará y procesará las respuestas de los Usuarios que así lo deseen para recomendarles el facultativo mejor adaptado a su situación, con redireccionamiento a la página de Teleconsultas de la aplicación para que los Usuarios elijan contratar una si así lo desean, tras la interacción con nuestro bot conversacional.

5. Política de precios

El precio del servicio de teleconsultas aparecerá en EUROS (€), con inclusión del IVA y cualesquiera otros impuestos aplicables.

Los conceptos adicionales, en su caso, serán indicados en la aplicación antes de iniciar el procedimiento de contratación.

6. Obligaciones

6.1. Nuestras obligaciones

H&T Hospitales, S.A., se compromete a:

a. Realizar eficaz y eficientemente los trámites para la ejecución del servicio.

b. Remitir a los Usuarios la información y documentación necesaria para la prestación del servicio.
c. Cumplir con estas obligaciones y cualesquiera otras aplicables.

6.2. Obligaciones de los Usuarios

Los Usuarios que contraten el servicio deben:

a. Pagar el precio especificado en el proceso de contratación. La falta de pago nos exime del cumplimiento de nuestras obligaciones.
b. Responder de la veracidad y autenticidad de los datos facilitados para la contratación.
c. Asumir las responsabilidades derivadas de los requisitos exigidos por estas Condiciones para ostentar la condición de los Usuarios, así como la falta de documentación necesaria para el pago.
d. Cumplir las obligaciones de estas Condiciones y cualesquiera otras aplicables, y asumir la responsabilidad derivada de su incumplimiento.

7. Desistimiento

En virtud del artículo 103.a) de la Ley General para la Defensa de los Consumidores y Usuarios, no será aplicable el derecho de desistimiento a los contratos de prestación de servicios en los que el servicio haya sido completamente ejecutado, cuando la ejecución haya comenzado, con previo consentimiento expreso del consumidor y usuario. En este sentido, el Usuario reconoce expresamente que es consciente de que, una vez el contrato haya sido completamente ejecutado habrá perdido su derecho de desistimiento.

Asimismo, en virtud del artículo 103.m) de la misma Ley, los Usuarios no tienen derecho de desistimiento de lo contratado en cuanto se ejecuten los servicios suscritos, entendiendo como tal el acceso, visualización o descarga de contenido y/o ejecución de lo contratado.

Como excepción, en caso de que no se ejecute el servicio, el Usuario podrá, en el plazo de catorce (14) días a partir de la fecha de contratación, ejercer su derecho de desistimiento sin tener que justificar los motivos de tal decisión ni pagar ninguna clase de penalización.

Una vez recibida la solicitud, se procederá al reintegro del precio abonado conforme a la modalidad de pago utilizada por el Usuario en la contratación

El Usuario también podrá comunicar al Titular su voluntad de desistir mediante el modelo que a continuación se facilita:

Modelo de formulario de desistimiento

A la atención de H&T Hospitales, S.A., con NIF A12345678, domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid) y dirección de correo electrónico clientes@h&thospitales.com;

Por la presente le comunico que desisto de mi contrato de servicio de teleconsulta, celebrado en fecha dd/mm/aa.

Nombre y apellidos:

Domicilio:

Fecha:

Firma:

Una vez pasados los 14 días sin haberse ejecutado el servicio suscrito, no habrá derecho de desistimiento.

8. Exclusión de responsabilidad

No seremos responsables por los daños y perjuicios causados al Usuario por causas imputables a este. Sólo seremos responsables por los daños y perjuicios causados como consecuencia de las contrataciones realizadas en la aplicación, siempre y cuando se deriven de una acción dolosa o culposa por nuestra parte.

A título enunciativo, no seremos responsables por:

a. La utilidad que para el Usuario tenga el servicio contratado.
b. Los daños provocados como consecuencia de la utilización del servicio, cuando no se han seguido las recomendaciones especificadas por nosotros.
c. El incumplimiento de nuestras obligaciones por motivos de fuerza mayor como huelgas, catástrofes naturales, etc.
d. El contenido y la forma de atención en las consultas por parte de los profesionales de H&T.

El Usuario que contrata bajo su propio riesgo. Nuestra actividad se limita a la ejecución de las tareas necesarias para la gestión y prestación del servicio.

En cualquier caso, la responsabilidad que asumimos frente al Usuario se limitará, como máximo y por cualquier concepto, al importe total percibido en contraprestación por la contratación del servicio, de conformidad con estas Condiciones.

9. Indemnización

Cualquier daño, perjuicio, pérdida o coste en que incurramos, derivado del incumplimiento de estas Condiciones o de cualesquiera otras que resultaren aplicables por parte del Usuario, deberá ser debidamente resarcido por el Usuario que lo causó.

10. Modificaciones

Las presentes Condiciones pueden ser modificadas y/o actualizadas en cualquier momento sin necesidad de previo aviso. Las modificaciones y/o actualizaciones entrarán en vigor desde el momento en que sean publicadas en la aplicación.

11. Otras cuestiones

11.1. Salvaguardia e interpretación

Si la Autoridad competente declarara ilegal, inválida o no ejecutable alguna de las disposiciones de estas Condiciones, tal disposición deberá pasar a ser interpretada de la manera más próxima a la intención original de aquélla. En cualquier caso, la declaración de la Autoridad competente con respecto de tal disposición o cláusula no perjudicará la validez de las demás.

11.2. Idioma

El idioma aplicable a nuestras Condiciones es el español. Si facilitamos versiones en otros idiomas será por cortesía y para mayor comodidad para los Usuarios, de forma que en caso de contradicción entre diferentes versiones idiomáticas, prevalecerá la versión en español.

11.3. Legislación y fuero

Las relaciones entre el Usuario y nosotros se regirán por la legislación española.

El fuero para la resolución de las eventuales controversias en torno a estas Condiciones dependerá de que el usuario ostente, o no, la condición de consumidor y/o usuario. Siendo consumidor y/o usuario, las controversias se someterán a los Juzgados y Tribunales del domicilio del Usuario. En caso contrario, las controversias se dirimirán en los Juzgados y Tribunales de la villa de Madrid.

Si el Usuario tuviera algún problema derivado de la contratación de nuestros servicios, podrá recurrir al sistema de resolución de litigios en línea de la Unión Europea, accesible a través del siguiente enlace: https://webgate.ec.europa.eu/odr/.

Anexo III: Política de Cookies

Esta Política de Cookies es aplicable a *H&TeHealth*, aplicación accesible a través de la URL https://es.h&tehealth.com, titularidad de H&T Hospitales, S.A., con NIF A12345678 y domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid) (en adelante, el Titular).

El acceso a nuestra aplicación y la navegación por esta supone el uso y descarga de cookies propias y de terceros en el dispositivo con que se acceda, para optimizar la navegación y analizar comportamientos durante esta y, así, analizar nuestros servicios.

1. ¿Qué son las cookies?

Las cookies son archivos de datos que se reciben en tu dispositivo y se usan para registrar las interacciones del Usuario con la aplicación, almacenando datos que podrán ser actualizados y recuperados del terminal. Estos archivos se almacenan en el dispositivo del Usuario y contienen datos, generalmente anónimos y no perjudiciales para el dispositivo. Se utilizan para recordar preferencias del Usuario, los datos de acceso, cuestiones relativas a la personalización de la página, etc.

Las cookies también pueden ser utilizadas para registrar información anónima acerca de cómo un visitante utiliza nuestra aplicación.

2. Consentimiento

Al acceder a la aplicación te ofreceremos información básica sobre el uso de cookies en *H&TeHealth* mediante un banner inferior, y te solicitaremos que otorgues tu consentimiento para su uso por nuestra parte haciendo clic en el botón "*Aceptar*".

No obstante, algunas cookies son necesarias para el funcionamiento de la aplicación y si se deniega su uso, el acceso a *H&TeHealth* podría quedar inhabilitado o no funcionar correctamente.

Además, por medio del panel de configuración de cookies, podrás elegir entre aceptar o rechazar todas las cookies, o hacerlo de forma granular, administrando tus preferencias con respecto de aquéllas.

En cualquier momento podrás retirar el consentimiento (véase apartado 4).

3. Cookies empleadas en *H&TeHealth*

Utilizamos las cookies estrictamente necesarias para analizar nuestros servicios.

En concreto, utilizamos los siguientes tipos de cookies:

Cookies de preferencia o personalización: para adaptar la aplicación a algunas características preestablecidas como el idioma, el navegador empleado o la región desde la que se accede.

Cookies técnicas: para proporcionar fluidez y comodidad durante la navegación, así como para garantizar su correcto funcionamiento y dotarla de mayor seguridad.

Cookies de análisis o medición: para obtener información para el análisis estadístico del uso que los Usuarios hacen de nuestra aplicación.

En el caso de que optes por no consentir el uso de cookies por nuestra parte, no descargaremos ninguna, salvo aquellas que la norma nos permite (como las cookies técnicas).

A continuación te mostramos un listado que agrupa las cookies de *H&TeHealth* indicando el tipo, origen, finalidad, y un enlace para que el Usuario pueda acceder a las Políticas de Cookies de los sitios de procedencia de las cookies.

COOKIES PROPIAS				
Cookies	**Origen**	**Información**	**Finalidad**	**Opt-out**
De personalización	*H&TeHealth*	Identificación y preferencias de navegación.	Almacenar variables de sesión y adaptar navegación según dichas variables.	Clic[112]
Analíticas	*H&TeHealth*	Navegación.	Conocer preferencias y hábitos de navegación y sugerir navegación conforme a ello.	Clic[113]
COOKIES DE TERCEROS				
Cookies	**Origen**	**Información**	**Finalidad**	**Opt-out**
Analíticas o de medición	Google Analytics (Google LLC)	Identificación, inicio y terminación de sesión, cálculo de permanencia, frecuencia de visita, localización, navegación, URL de procedencia, medición de recogida de datos.	Obtener estadísticas de hábitos de visita y navegación, conocer preferencias de opciones variables y adaptar la navegación, hacer sugerencias de navegación, intercambiar información con otras cookies de Google.	Clic

Además de las cookies, podemos utilizar "píxeles de seguimiento" (*web beacons* o *pixel tags*), imágenes transparentes integradas en la aplicación que permiten verificar aspectos como el número de visitantes de una página o la configuración técnica del navegador con que se accede a la aplicación. Las finalidades de estos píxeles son los mismos que se han descrito en la tabla.

4. Cambiar la configuración de cookies o revocar el consentimiento

En cualquier momento podrás retirar tu consentimiento al uso de cookies. Para ello, podrás:

Administrar tus preferencias en el panel de configuración que ponemos a tu disposición en la aplicación.

[112] Enlace a la Política de Privacidad de la aplicación.
[113] Enlace a la Política de Privacidad de la aplicación.

Desactivar la descarga de cookies en el navegador que utilices habitualmente. Te facilitamos a continuación un listado de enlaces para la gestión de cookies en los navegadores más comunes:

Safari: https://support.apple.com/kb/ph21411?locale=es_ES.

Google Chrome: https://support.google.com/chrome/answer/95647?hl=es.

Internet Explorer: http://windows.microsoft.com/es-es/internet-explorer/delete-manage-cookies#ie=ie-11.

Microsoft Edge: https://privacy.microsoft.com/es-es/windows-10-microsoft-edge-and-privacy.

Mozilla Firefox: http://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-que-los-sitios-we.

Opera: https://help.opera.com/en/latest/web-preferences/#cookies.

Estos navegadores se someten a actualizaciones y modificaciones periódicas por parte de sus respectivos titulares, por lo que si los enlaces anteriores no estuvieran actualizados, si tu navegador no está entre ellos, o si no hallas la forma de gestionar cookies, consulta con el sitio web oficial del titular correspondiente o ponte en contacto con nosotros.

Ante cualquier duda con respecto de las cookies, no dudes en escribirnos a: rgpd@h&thospitales.com.

***

Cláusula informativa (primera capa) de Cookies:

Utilizamos cookies propias y de terceros para analizar nuestros servicios. Puedes aceptar todas las cookies pulsando el botón "*Aceptar*" o configurarlas o rechazar su uso haciendo clic aquí[114]. Para más información, consulta nuestra Política de Cookies[115].

[114] Enlace al panel de configuración de cookies de la aplicación.
[115] Enlace a la Política de Cookies de la aplicación.

Anexo IV: Política de Privacidad

Responsable del tratamiento

El Responsable del tratamiento de los datos es H&T Hospitales, S.A., con NIF A12345678 (en adelante, el Responsable) y domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid), titular de la aplicación *H&TeHealth*.

Esta Política de Privacidad regula todo lo relativo a la recogida y tratamiento de todos aquellos datos personales que sean facilitados por los Usuarios cuando accedan, naveguen o hagan uso de las funcionalidades de *H&TeHealth*.

Recogida de datos, finalidades, base de legitimación y conservación

a. Contacto: el Usuario puede contactar con el Responsable mediante el formulario de contacto de la aplicación. A tal fin, se deberán facilitar datos identificativos, de contacto y asunto a tratar. Los datos se utilizarán para tramitar la consulta y contactar con el Usuario. La base jurídica del tratamiento se sustenta en el consentimiento del Usuario. Los datos serán conservados durante 1 año, salvo que sean aplicables otros plazos.
b. Registro: para registrarse en la aplicación, el Usuario tendrá que facilitar sus datos identificativos y de contacto, para la tramitación del registro y permitir el acceso a la contratación de servicios en la aplicación. La base jurídica del tratamiento se sustenta en la ejecución de un contrato fundado en las Condiciones Generales de Uso[116]. Los datos serán conservados mientras el Usuario se encuentre registrado en *H&TeHealth*.
c. Contratación: el Usuario puede contratar el servicio de teleconsulta de *H&TeHealth*. Para ello, deberá facilitar sus datos identificativos y de contacto, así como aquellos otros datos necesarios para tramitar la contratación, como datos bancarios o de tarjetas de crédito. La base jurídica del tratamiento se sustenta en la ejecución del contrato. Los datos serán conservados durante el tiempo necesario para cumplir el contrato y, en todo caso, hasta 5 años más por cuestiones tributarias y para depurar eventuales responsabilidades, salvo que sean aplicables otros plazos.
d. Cookies: las cookies pueden ser bloqueadas o deshabilitadas en cualquier momento a través de las opciones de configuración del navegador. Si desea más información puede consultar nuestra Política de Cookies[117]. La base jurídica del tratamiento se sustenta en el consentimiento del Usuario.
e. Publicidad y marketing: si el Usuario lo autoriza expresamente, el Responsable podrá enviarle publicidad de sus servicios. La base jurídica del tratamiento se sustenta en el consentimiento del Usuario. Los datos se conservarán durante el tiempo en que el Usuario permanezca suscrito en el sistema de envío de publicidad y no haya revocado su consentimiento. En cualquier momento puede revocar su consentimiento mediante los enlaces facilitados o escribiéndonos a rgpd@h&thospitales.com.

[116] Enlace al Aviso Legal y Condiciones Generales de Uso de la aplicación.
[117] Enlace a la Política de Cookies de la aplicación.

Comunicaciones a terceros

No comunicaremos los datos de los Usuarios a terceros.

Ejercicio de derechos

El Usuario podrá revocar el consentimiento para el tratamiento y ejercitar sus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento, comunicándolo al Responsable través en rgpd@h&thospitales.com, o en la dirección postal indicada más arriba. Cuando existan dudas acerca de su identidad, el Responsable podrá solicitar al Usuario una acreditación de aquélla mediante documento oficial, para evitar el acceso no autorizado a sus datos.

Asimismo, el Usuario podrá presentar una reclamación ante la Agencia Española de Protección de Datos para obtener la tutela de sus derechos.

Modificaciones

El Responsable se reserva el derecho de modificar la política de privacidad en cualquier momento, observando la legislación vigente y previa comunicación a los interesados sobre este hecho.

Idioma

El idioma aplicable a esta política es el español. Si se facilitan versiones en otros idiomas será por cortesía y para mayor comodidad de los Usuarios, de forma que en caso de contradicción entre diferentes versiones idiomáticas, prevalecerá la versión en español.

Anexo V: Política de Privacidad del Chatbot

Responsable del tratamiento

El Responsable del tratamiento de los datos recabados es H&T Hospitales, S.A., con NIF A12345678 (en adelante, el Responsable) y domicilio en Calle Diego de Velázquez nº1, 28223 de Pozuelo de Alarcón (Madrid), titular de la aplicación *H&TeHealth*.

Esta Política de Privacidad regula la recogida y tratamiento de todos aquellos datos personales facilitados por los Usuarios a través de la funcionalidad de Chatbot de *H&TeHealth*, que realiza un cuestionario por el que elabora una recomendación de elección de facultativo en función del posible cuadro sintomatológico del Usuario, basado en la información por este facilitada y, en su caso, concertar una teleconsulta.

Recogida de datos, finalidades, base de legitimación y conservación

Cuestionario: se solicitarán los siguientes datos:

a. Datos relativos a características personales y circunstancias laborales y sociales:
    i. Sexo (Hombre / Mujer).
    ii. Edad.
    iii. Profesión y datos relativos a esta (naturaleza activa / sedentaria / interior / exterior / sector).
    iv. Tabaco (consumidor / no consumidor)
    v. Consumo de alcohol y periodicidad de este.
b. Datos relativos a la salud:
    i. Existencia o no de familiares enfermos de alguna clase de cáncer y grado de parentesco con aquéllos, en su caso.
    ii. Existencia o no de intervenciones quirúrgicas anteriores en relación con la piel.
    iii. Padecimiento de Virus de Hepatitis B o C.
    iv. Manifestación del dolor, en su caso (localizado o extendido).
    v. Antigüedad del dolor.
    vi. Frecuencia del dolor.
    vii. Existencia o no de lunares y/o manchas de nacimiento.
    viii. Grado de asimetría en el lunar o mancha de nacimiento.
    ix. Forma de los bordes (irregulares, desiguales, borrosos).
    x. Color del lunar o mancha (marrón o negro, zonas rosadas, rojo, blanco, azul).
    xi. Diámetro del lunar o mancha (mayor o menor de 0´6 cm).
    xii. Evolución del lunar o mancha (cambios en tamaño, forma o color).

La base jurídica del tratamiento de los datos se sustenta en el consentimiento del Usuario.

El plazo de conservación de los datos será de 1 año, salvo que sean aplicables otros plazos. Asimismo, los datos serán conservados de forma agregada para fines estrictamente estadísticos.

Teleconsulta: si se acepta la realización de una teleconsulta, se redirigirá a la correspondiente página en la aplicación, siendo aplicable la Política de Privacidad[118] de aquélla.

Ejercicio de derechos

El Usuario podrá revocar el consentimiento para el tratamiento y ejercitar sus derechos de acceso, rectificación, supresión, portabilidad, oposición y limitación al tratamiento, comunicándolo al Responsable través en rgpd@h&thospitales.com, o en la dirección postal indicada más arriba. Cuando existan dudas acerca de su identidad, el Responsable podrá solicitar al Usuario una acreditación de aquélla mediante documento oficial, para evitar el acceso no autorizado a sus datos.

Asimismo, el Usuario podrá presentar una reclamación ante la Agencia Española de Protección de Datos para obtener la tutela de sus derechos.

Modificaciones

El Responsable se reserva el derecho de modificar la política de privacidad en cualquier momento, observando la legislación vigente y previa comunicación a los interesados sobre este hecho.

Idioma

El idioma aplicable a esta política es el español. Si se facilitan versiones en otros idiomas será por cortesía y para mayor comodidad de los Usuarios, de forma que en caso de contradicción entre diferentes versiones idiomáticas, prevalecerá la versión en español.

[118] Enlace a la Política de Privacidad de la aplicación.

Anexo VI: Cuestionario para Encargados

Le remitimos el presente cuestionario con motivo de los trabajos de adaptación al Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril, 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 (RGPD). Esta norma obliga a las empresas a contratar únicamente con proveedores "*que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas*", en cumplimiento del marco regulatorio y de los requisitos del RGPD.

Le rogamos que complete el cuestionario y nos lo remita a rgpd@h&thospitales.com.

1. **Descripción del servicio.** Describa brevemente el tipo de servicio que nos presta, con las tipologías de datos que incluye.
2. **Obligaciones legales.**
    a. **¿Ha nombrado un Delegado de Protección de Datos?** Si su empresa está obligada a nombrar esta figura, le rogamos que nos indique sus datos. Si no, indíquenos una persona de contacto para la gestión de asuntos relacionados con la protección de datos.
    b. **¿Subcontratan el servicio que nos prestan?** La delegación de cualquier servicio, total o parcialmente, en personas ajenas a su empresa (incluyendo el hosting) debe ser comunicada al Responsable del tratamiento, *H&T Hospitales*, indicando las actividades concretas que serán delegadas y la existencia, o no, de contratos firmados con tales personas. En caso afirmativo, será necesario trasladar el presente cuestionario también a los subcontratistas.
    c. **¿Cómo atienden los derechos de los interesados?** El RGPD obliga a los Encargados del tratamiento a asistir a sus clientes en supuestos de ejercicio de derechos por parte de los interesados.
    d. **¿Cuentan sus empleados y colaboradores con información acerca del cumplimiento del RGPD?** Cursos, manuales o guías que se hayan podido facilitar, con especial atención a las obligaciones de confidencialidad.
    e. **¿Cómo podríamos supervisar su grado de cumplimiento de estas obligaciones?** Conforme a la normativa, Vds. deben poner a nuestra disposición documentación acreditativa del cumplimiento del RGPD, permitiéndonos auditar e inspeccionar tal cumplimiento.
3. **Medidas de seguridad.**
    a. **Los datos que les facilitamos para prestar sus servicios, ¿se tratan en la nube?** Indíquenos la herramienta elegida y dónde podemos encontrar información acerca de su cumplimiento del RGPD.
    b. **Los datos que les facilitamos para prestar sus servicios, ¿se tratan en sus servidores?** En caso afirmativo, necesitamos información sobre controles de acceso a aquéllos, medidas de protección, procesos de copias de seguridad, etc.
    c. **Los accesos a la información, ¿están adecuadamente limitados?** Necesitamos confirmar si el acceso a los datos se limita a las personas estrictamente necesarias, con las medidas implementadas para evitar accesos no autorizados.

d. **Los equipos de sus empleados con acceso a nuestros datos, ¿están securizados?** Necesitamos saber si cuentan con antivirus, permisos, accesos controlados por claves, bloqueos, copias de seguridad, etc.
e. **¿Es posible el acceso remoto a los datos personales que tratan por cuenta de nosotros?** Si es así, indique las medidas implementadas para evitar el acceso no autorizado.
f. **¿Se verifica regularmente el cumplimiento de estas medidas?** Si es así, explique el procedimiento de verificación.
g. **¿Cuentan con certificaciones en materia de gestión de la seguridad de la información?** Por ejemplo, ISO 27001.
h. **¿Cómo nos informarán en caso de que se produzca una brecha de seguridad en sus sistemas?** Describa el protocolo aplicable.

4. **Medidas de responsabilidad proactiva.**
   a. **¿Tienen un registro de actividades de tratamiento?** Si es así, remítanos una copia de aquellas páginas correspondientes a los tratamientos relativos a nuestra empresa.
   b. **¿Han analizado los riesgos de los tratamientos que realizan para nosotros?** Si es así, remítanos una copia de aquellas páginas correspondientes a los tratamientos relativos a nuestra empresa.
   c. **¿Cómo han implementado las obligaciones de protección de datos desde el diseño y por defecto?** Este punto resulta de especial interés en el caso de que pongan a nuestra disposición una herramienta tecnológica que sirva para tratar datos personales. Indíquenos, en su caso, las opciones que incorpora la herramienta para cumplir con el RGPD.

Bibliografía y lista de referencias

Aleixandre Benavent, R., Ferrer Sapena, A. y Peset Mancebo, M. F. (2010). Informatización de la historia clínica en España. *El profesional de la información*, Vol. 19 (nº3).

Álvarez Hernando, J. (2011). *Guía práctica sobre Protección de datos: cuestiones y formularios*. Madrid: Lex Nova.

Anónimo. (30 de marzo de 2020). La OMS advierte de que el colapso sanitario por el coronavirus puede aumentar las muertes de enfermedades tratables. *Infosalus*.

Anónimo. (28 de marzo de 2016). Una inteligencia artificial se vuelve racista, antisemita y homófoba en menos de un día en Twitter. *El Mundo*.

Barrio Andrés, M. (2017). *Fundamentos del Derecho de Internet*. Madrid: Centro de Estudios Políticos y Constitucionales.

Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*.

Cortés Saavedra, J. M. (2017). El proceso de "compliance" y el responsable de seguridad. *Seguritecnia* (nº442).

Crocetti, P. (24 de julio de 2019). Tipos de copias de seguridad explicados: incremental, diferencial o de espejo. *SearchDataCenter*.

Cuena Casas, M. (28 de febrero de 2019). Los riesgos para los consumidores y usuarios en la contratación a través de plataformas intermediarias en línea. *Hay Derecho – Expansión*.

Edmunds, M.; Tuckson, R.; Lewis, J. y Atchinson, B. (2017). An Emergent Research and Policy Framework for Telehealth. *eGEMs (Generating Evidence & Methods to improve patient outcomes)*, Vol. 5.

Gil, E. (2015). Big data, privacidad y protección de datos. *Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado*.

Gómez, S.; Arias, J.D. y Agudelo, D. (2012). Cripto-análisis sobre métodos clásicos de cifrado. *Scientia et Technica*, Vol. 2 (nº50).

Koomen, M. (2019). The Encryption Debate in the European Union. *Carnegie Endowment for International Peace*.

Laukyte, M. (2018). Robots y Sanidad. En *Sociedad Digital y Derecho* (p. 865-878). Madrid: Publicaciones Oficiales BOE.

Letzter, R. (23 de mayo de 2016). This software that helps predict criminal behavior is under fire for having a "racist" algorithm. *Business Insider*.

Lloret, J.; Parra, L.; Taha, M. y Tomás, J. (2017). An architecture and protocol for Smart continuous eHealth monitoring using 5G. *Computer Networks*, Volume 129, Part 2

López, C. Mª. (14 de abril de 2020). Los puntos cardinales de la telemedicina en tiempos de Covid-19. *Gaceta Médica*.

López-Monís, M. (2003). Ámbito de aplicación de la nueva Ley de Servicios de la Sociedad de la Información y de comercio electrónico. En *Derecho de Internet: la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico* (pp. 25-64). Madrid: Aranzadi.

Magro Servet, V. (2013). Responsabilidad por culpa in vigilando. *Revista de Jurisprudencia LEFEBVRE-El Derecho, nº2*.

Márquez Lobillo, P. (2007). Obligaciones y responsabilidades de los empresarios y los profesionales en la sociedad de la información. En *Empresarios y profesionales en la sociedad de la información* (pp. 287-407). Madrid: Edersa.

Marrero Pérez, M. (2011). Implicaciones Éticas Asociadas al Uso de la Telemedicina. Revista eSalud, Vol. 7 (nº28).

Martínez Zaporta, E. (2008). Telemedicina y responsabilidad patrimonial de la Administración Sanitaria. *Revista Española de Administración Sanitaria*, Vol. 16 (nº1).

Mercado Carmona, C. (2005). La eSalud y el Derecho. *Revista eSalud*, Vol. 1 (nº2).

Moore, S. (19 de febrero de 2018). Gartner Says 25 Percent of Customer Service Operations Will Use Virtual Customer Assistants by 2020. *Gartner Press Releases*.

Mujica, M. y Álvarez, Y. (2009). El Análisis de Riesgo en la seguridad de la información. *Publicaciones en Ciencias y Tecnología*, Vol. 4 (nº2).

Real, P. (25 de julio de 2018). Próxima frontera digital: el comercio conversacional. *El País*.

Reyes Rico, L. (13 de agosto de 2019). Límites de la normativa de protección de datos a la creación de perfiles con fines comerciales. *LegalToday*.

Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales: el remedio indemnizatorio del artículo 82 RGPD. *Revista de Derecho Civil*, Vol. V (nº4).

Sánchez, L. J. (20 de octubre de 2018). Configurar un chatbot supone ya aplicar para la empresa creadora los nuevos principios de privacidad que exige el RGPD. *Confilegal*.

Singh, S. (2000). *Los códigos secretos*. Madrid: Debate.

Valín López, M. (2018). Apuntes sobre el Delegado de Protección de Datos y la Administración General de Euskadi. *Revista Vasca de Gestión de Personas y Organizaciones Públicas* (nº 14).

Villaseca, M. (2018). El delegado de protección de datos. *I+S: Revista de la Sociedad Española de Informática y Salud* (nº 127).

Weizenbaum, J. (1976). *Computer power and human reason: from judgment to calculation*. Nueva York: W. H. Freeman and Company.

Otros

AEPD. (2017). *Código de buenas prácticas en protección de datos para proyectos Big Data*.

AEPD. (2018). *Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.*

AEPD. (2018). *Informe sobre políticas de privacidad en Internet*.

AEPD. (2018). *Guía para la gestión y notificación de brechas de seguridad*.

AEPD. (2018). *Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD.*

AEPD. (2019). *Guía para pacientes y usuarios de la Sanidad*.

AEPD. (2019). *Guía sobre el uso de las cookies*.

AEPD. (2019). *Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*.

American Cancer Society medical and editorial content team. (22 de abril de 2020). Telemedicina y telesalud.

Autoridad Catalana de Protección de Datos. (2019). *El encargado del tratamiento en el Reglamento General de Protección de Datos (RGPD)*.

Centro Criptológico Nacional. (2011). *Guía de Seguridad: Esquema Nacional de Seguridad, valoración de los sistemas*.

CGCOM. (Julio de 2011). *Código de Deontología Médica: Guía de Ética Médica*.

CNIL. (2020). *GDPR Guide for Developers*.

Comisión Europea. (Julio de 2016). *Guidelines on the qualification and clasiffication of stand alone software used in healthcare within the regulatory framework of medical devices* (MEDDEV 2.1/6).

CPME. (abril de 1997). *Ethical Guidelines in telemedicine* (CP 97/033).

ECIJA & Chatbot Chocolate. (2018). *Guía legal chatbots: aspectos jurídicos y de mercado*.

Fundación Salud 2000. (septiembre de 2012). *Telemedicina: bases para la futura regulación de un mercado emergente* (Informe del experto Nº5).

GT29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales* (WP 136).

GT29. (2010). *Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"* (WP 169).

GT29. (2014). *Dictamen 05/2014 sobre técnicas de anonimización* (WP 216).

GT29. (2016). *Directrices sobre los delegados de protección de datos (DPD)* (WP 243).

GT29. (2017). *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* (WP 259).

GT29. (2017). *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679* (WP 248).

INCIBE-CERT. (2018). *Copias de seguridad: una guía de aproximación para el empresario*.

INCIBE-CERT. (2018). *Uso de técnicas criptográficas*.

Informe del Gabinete Jurídico de la AEPD Nº2009/0467, de 29 de enero de 2010.

NASA. (6 de abril de 2020). *NASA and Telemedicine*.

Norma Internacional ISO/IEC 29100 (2011). *Tecnología de la Información – Técnicas de seguridad – Marco de privacidad*. Suiza: ISO.

OMS. (13 de enero de 2011). *Global Observatory for eHealth series - Volume 2*.

Organización para la Cooperación y el Desarrollo Económicos. (2002). *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad*.

Panel for the Future of Science and Technology of the European Parliament. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (PE 641.530).

PwC EU Services, para la Comisión Europea. (4 de septiembre de 2019). *Architecture for public service chatbots*.

Anexo de legislación

Directiva 93/42/CEE del Consejo, de 14 de junio de 1993, relativa a los productos sanitarios (DOCE núm. L 169, de 12 de julio de 1993).

Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas (DOCE núm. L 204, de 21 de julio de 1998).

Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DOCE núm. L 8, de 12 de enero de 2000).

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DOCE núm. L 178, de 17 de julio de 2000).

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DOCE núm. L 201, de 31 de julio de 2002)

Versión consolidada del Tratado de Funcionamiento de la Unión Europea (DOUE núm. C 83, de 30 de marzo de 2010).

Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DOUE núm. L 88, de 4 de abril de 2011).

Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DOUE núm. L 241, de 17 de septiembre de 2015).

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 y por el que se deroga la Directiva 95/46/CE (DOUE núm. L 119, de 4 de mayo de 2016).

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DOUE núm. L 194, de 19 de julio de 2016).

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE (DOUE núm. L 295, de 21 de noviembre de 2018).

Ley 14/1986, de 25 de abril, General de Sanidad (BOE núm. 102, de 29 de abril de 1986).

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE núm. 166, de 12 de julio de 2002).

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 (BOE núm. 274, de 15 de noviembre de 2002).

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE núm. 25, de 29 de enero de 2010).

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (BOE núm. 287, de 30 de noviembre de 2007).

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 (BOE núm. 17, de 19 de enero de 2008).

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (BOE núm. 218, de 8 de septiembre de 2018).

Otros

Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, de 8 de octubre de 1997, sobre el fomento de la seguridad y la confianza en la comunicación electrónica – Hacia un marco europeo para la firma digital y el cifrado (COM 97/503).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 4 de noviembre de 2008, "La telemedicina en beneficio de los pacientes, los sistemas sanitarios y la sociedad" (COM 2008/689).

Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 26 de agosto de 2010, "Una Agenda Digital para Europa", (COM 2010/245).

Propuesta de la Comisión Europea de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (COM 2017/10).

Reglamento de Ejecución (UE) 2018/151 de la Comisión, de 30 de enero de 2018, por el que se establecen normas para la aplicación de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo en lo que respecta a la especificación de los elementos que han de tener en cuenta los proveedores de servicios digitales para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información, así como de los parámetros para determinar si un incidente tiene un impacto significativo (DOUE núm. L 26, de 31 de enero de 2018).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 25 de abril de 2018, relativa a la consecución de la transformación digital de la sanidad y los servicios asistenciales en el Mercado Único Digital, la capacitación de los ciudadanos y la creación de una sociedad más saludable (COM 2018/233).

Anexo de jurisprudencia

Sentencia del Tribunal de Justicia de la Unión Europea de 11 de abril de 2000 (asuntos acumulados C-51/96 y C-191/97).

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera), de 7 de mayo de 2009 (asunto C-553/07).

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Cuarta), de 3 de septiembre de 2015 (asunto C-110/14).

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Cuarta), de 7 de diciembre de 2017 (asunto C-329/16).

Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 1 de octubre de 2019 (asunto C-673/17).

Sentencia del Tribunal General de la Unión Europea (Sala Sexta), de 3 de diciembre de 2015 (asunto T-343/13).

Sentencia del Tribunal Supremo 452/1997, de 27 de enero de 1997.

Sentencia del Tribunal Superior de Justicia de Castilla-La Mancha (Sala de lo Social), de 9 de febrero de 2017 (Nº de Recurso 1697/2017).

Otros

Resolución de la Agencia Española de Protección de Datos (Procedimiento PS/00127/2019).

Resolución de la Agencia Española de Protección de Datos (Procedimiento PS/00184/2019).

Resolución de la Agencia Española de Protección de Datos (Procedimiento PS/00262/2019).

Resolución de la Agencia Española de Protección de Datos (Procedimiento PS/00299/2019).