- **Expediente N.º: EXP202413408**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La Agencia Española de Protección de Datos ha tenido conocimiento a través de una denuncia efectuada con fecha 3 de septiembre de 2024, de ciertos hechos que podrían vulnerar la legislación en materia de protección de datos, en relación con las deficiencias de seguridad del sistema de recopilación digital de datos por parte de la compañía denunciada, HM HOSPITALES 1989, S.A. con NIF A79325858 (en adelante, HMH) y que estaría siendo utilizado por distintos centros hospitalarios.

Según la parte denunciante, en la puesta en funcionamiento del sistema de recolección de datos y firma digital la empresa denunciada estaría recopilando una cantidad de información excesiva e innecesaria para confirmar la identidad de los receptores de documentación, incluyendo en el proceso datos tales como el dispositivo utilizado, el IMEI del dispositivo, la geolocalización y otros, cuando sería suficiente, a su juicio, con una mera firma digital para validar la identidad del receptor.

Asimismo, según se indica en la denuncia, HMH elaboró una Evaluación de Impacto Protección de Datos (en adelante, EIPD) con posterioridad a la puesta en funcionamiento del sistema de recolección de datos y firma digital, a pesar de que era obligatorio realizarla con anterioridad, como le advirtió la empresa externa encargada de la validación de las firmas digitales.

Junto al escrito aporta la siguiente documentación:

a) Contrato de Prestación del Servicio ViDSigner entre la empresa reclamada y una tercera empresa externa (******EMPRESA.1***), con fecha de 19 de junio de 2018, incluye las condiciones generales del servicio.

Se destaca el siguiente texto del contrato relacionado:

De su apartado 2 "*DESCRIPCIÓN DEL SERVICIO*" que (…) "*ViDSigner es un Servicio integral de firma electrónica operado por ViD como prestador de servicios de confianza que se adapta a cada caso de uso en función de la tipología del firmante, la capacidad tecnológica de las partes o los requerimientos legales o de seguridad requeridos en diferentes modalidades: firma presencial (biométrica), remota (basada en certificados), local con dispositivo seguro de creación de firma (dnie/smartcard) o automatizada (basada en certificados de sello).*
El Servicio de firma de ViDSigner puede utilizarse de forma independiente o combinados entre sí.

En la modalidad presencial, el proceso firma se basa en la utilización de tecnología de firma electrónica manuscrita y emplea elementos de gran valor como la obtención de elementos biométricos de la firma codificados según estándar ISO, certificados digitales y sellos de tiempo, cifrado de los datos biométricos con claves custodiadas en sede notarial, entre otros. En la modalidad de firma remota se permite que los usuarios puedan firmar documentos a través de una app desde sus dispositivos Smartphone/tablets o bien accediendo a través de una página web desde el PC, laptop o dispositivo móvil mediante un sistema de centralización de claves y certificados digitales que delega la complejidad de la generación/gestión de las firmas en ViD como prestador del Servicio. Dependiendo de la configuración del Servicio, las firmas remotas realizadas con ViDSigner tendrán la consideración de firmas cualificadas o avanzadas de acuerdo con el Reglamento UE 910/2014.

La modalidad de firma local aprovecha las nuevas funciones de conectividad del DNIe 3.0 o una smartcard con capacidades equivalentes para permitir la generación de firmas cualificadas desde un smartphone a través de la tecnología NFC.

Por último, el Servicio de firma automatizada permite la firma de documentos en entornos no presenciales de forma totalmente desasistida a partir de un certificado digital alojado y custodiado remotamente".

De su apartado 5, en Anexo I, *"Obligaciones de EL CLIENTE*" se indica que (…) "*Corresponde al CLIENTE, como responsable de tratamiento: 5.2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por ViD*" (…)

b) Informe de Evaluación de Impacto en la Protección de Datos sobre la recopilación de datos a la hora de la recepción de documentación de forma digital, elaborado por la empresa reclamada, con fecha de 16 de noviembre de 2021.

En este informe se indica que (…) *"resulta CONVENIENTE realizar una EIPD, pues el tratamiento cumple 3 de los requisitos recogidos en la lista orientativa de tipos de tratamiento que requieren EIPD publicada por la AEPD*" (…) ya que dicho tratamiento (…) "*implica el uso de datos biométricos con el propósito de identificar de manera única a una persona física*", toda vez que "*La firma que realizaran los interesados sobre tabletas o smartphones puestos a disposición de HM HOSPITALES para la recogida/captura, puedan recoger aspectos biométricos de la firma, como son el trazo, la presión o la velocidad, que juntos hacen que ésta sea una firma única, asociada inequívocamente a una persona*". (…) Además, (…) "*Puede darse tratamiento de datos a gran escala*" (…) Y (…) "*El servicio VIDsigner BIO el proceso de firma se basa en la utilización de la tecnología de firma electrónica manuscrita y emplea elementos de gran valor como la obtención de datos biométricos de la firma codificados según estándar ISO, certificados digitales y sellos de tiempo, cifrado de los datos biométricos con claves custodiadas en sede notarial, entre otros*" (…)

En el apartado 3 de dicho Informe "*DESCRIPCIÓN DEL TRATAMIENTO*" se señala que:

"3.1. *Identificación y antecedentes. Identificación y descripción.*

El tratamiento se corresponde con el de firma manuscrita electrónica.

La descripción del tratamiento consiste en la recogida de los datos biométricos de la firma manuscrita del firmante en un documento mediante el servicio VIDsigner BIO utilizando un dispositivo electrónico tipo "Tablet".

Dichos datos son la posición, tiempo y presión de los rasgos de firma.

La finalidad del tratamiento es que HM HOSPITALES o el interesado puedan identificar, con las máximas garantías de seguridad jurídica, al autor de la firma y demostrar, en caso de litigio, la autoría y autenticidad de la firma." (…)

Constando como "Datos personales objeto de tratamiento" los "*Datos personales de cualquier naturaleza, básicos y especiales, incluidos en los documentos firmados, y que pueden clasificarse en:*

> *- Datos identificativos, que son utilizados para identificar a las personas que firman los documentos.*
> *- Datos incluidos en los documentos firmados, los cuales son útiles para ejecutar la prestación del servicio de firma electrónica, pero no para identificar las personas que firman los documentos." (…)*

Y como "*Finalidad del tratamiento*" la de "*digitalizar el proceso de digitalización de firma manuscrita, es decir, de captura y obtención de firma manuscrita a través de dispositivos electrónicos, en lugar del papel*" (…)

Conforme al apartado 4 de dicho Informe "*ANÁLISIS DEL TRATAMIENTO*" figura en dicho Informe el Ciclo de vida de los datos objeto del tratamiento consta de las siguientes fases:

> *"Fase 1: entrada o captura de los datos biométricos.*
>
> *La captura de la firma manuscrita a través de dispositivo electrónico (tabletas) usando el servicio VIDsigner Bio, puede tener lugar de origen en uno de los siguientes:*
>
> *- Dependencias de HM HOSPITALES.*
> *- Dependencias del lugar donde el firmante esté situado Respecto a los datos personales recopilados, se identifican tres categorías de datos personales en la fase de entrada de datos:*
>
> • *Datos personales básicos de identificación de los firmantes:*
> *- nombre y apellidos (obligatorio).*
> *- NIF (obligatorio).*
> *- correo electrónico (opcional).*
> *- biométricos de los rasgos de comportamiento de la firma manuscrita (obligatorio): posición, tiempo y presión de los rasgos de la firma.*

• *Datos personales de cualquier naturaleza, básicos y especiales, incluidos en los documentos firmados:*

- *Identificación*
- *económicos y seguros*
- *características personales*
- *circunstancias sociales*
- *salud - origen étnico o racial*
- *convicciones religiosas o filosóficas*
- *genéticos*
- *biométricos*
- *vida sexual u orientación sexuales*

Fase 2: clasificación de los datos.

En función de la utilidad del tratamiento, los datos personales se pueden clasificar en dos categorías:

- Datos que son útiles exclusivamente para identificar a las personas que firman los documentos.

- Datos que están incorporados en los documentos firmados, los cuales son útiles para ejecutar la prestación del servicio de firma electrónica, pero no para identificar las personas que firman los documentos.

Fase 3: uso o explotación de los datos.

Las aplicaciones de HM HOSPITALES que consumen el servicio de VIDsigner BIO se comunican con el servicio utilizando una API REST.

Esta API REST está asegurada bajo el canal SSL con un certificado SSL para que todas las comunicaciones entre las referidas aplicaciones y VIDsigner BIO estén cifradas.

Así, en el servicio de firma VIDsigner BIO la aplicación del responsable se comunica con la API REST para enviar a firmar el documento en formato PDF al dispositivo de captura de firma junto a la información de identificación del firmante: nombre y apellidos, NIF y correo electrónico (no obligatorio).

La APP VIDsigner BIO es responsable de mostrar el documento al usuario y recabar la firma que procesará el Servicio de Cloud." (…)

Fase 4: almacenamiento. Almacenamiento en la nube (Azure).

- Almacenamiento de la base de datos. La información del firmante se almacena en una base de datos durante el proceso de firma.

El acceso a esta base de datos está asegurado de dos maneras:

• *IP: Sólo los servidores VIDsigner pueden acceder a la base de datos*
• *Contraseña: Se requiere una contraseña para acceder a los datos almacenados en la base de datos. Además, la información de la base de datos está protegida mediante TDE (encriptación transparente de*

datos), por lo que, aunque se acceda a la base de datos, la información sigue siendo confidencial.

- Almacenamiento de documentos. Los documentos se almacenan en un blob storage que permite guardar grandes cantidades de documentos de cualquier tamaño. El acceso a este almacenamiento está protegido, por lo que sólo los servidores VIDsigner pueden acceder a ellos.
Esta información se almacena cifrada, así que incluso si se accede al almacenamiento la información permanece confidencial.
Proceso de almacenamiento del documento firmado con el servicio VIDsigner.

Todos los datos obtenidos, una vez realizada la operación de firma mediante la herramienta VIDsigner BIO, se cargan, a través de la API correspondiente, en los sistemas centrales de Azure, los cuales quedan almacenados temporalmente en dos repositorios:
- En la base de datos del sistema (cifrado).
- En el servicio de "storage" del sistema (cifrado).

Una vez enviado el documento a la APP VIDsigner, dicho documento mismo puede firmarse, no firmarse, o rechazarse." (…)

Fase 5: destrucción de los datos. Una vez finalizado el proceso de descarga del documento por HM HOSPITALES, Validated elimina el documento y la información del firmante de sus sistemas y el HM HOSPITALES conserva el documento en sus sistemas de información durante el tiempo necesario para poder garantizar el derecho del responsable de demostrar, ante la autoridad judicial o administrativa competente, la autoría y autenticidad de la firma realizada en su documento presentado por un ciudadano al responsable del tratamiento con el objeto de evitar cualquier responsabilidad que se pudiera derivar de reclamaciones o acciones interpuestas ante dicho responsable" (…)

SEGUNDO: Con fecha de 2 de octubre de 2024 la Presidencia de la Agencia Española de Protección de Datos instó a la Subdirección General de Inspección de Datos (SGID) a iniciar las actuaciones previas de investigación a las que se refiere el artículo 67 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD) para investigar los hechos denunciados, en relación con HMH.

TERCERO: La SGID procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

El objeto de las actuaciones de investigación se ha centrado en determinar los datos que se tratan por la parte reclamada en el sistema de firma digital que emplea en sus actividades de tratamiento y si los datos tratados requerían o no una EIPD.

En fecha 24 de septiembre de 2025, HMH presentó escrito de contestación a requerimiento de esta Agencia en el que, entre otros aspectos, manifestó lo siguiente:

Con carácter previo, realiza una serie de aclaraciones en relación con los sistemas DOCTORIS y +FIRMA:

I. *(…) "Introducción: Sistemas DOCTORIS y +FIRMA*

En el marco de la actividad asistencial desarrollada por HM Hospitales, la gestión de la información clínica se articula a través de DOCTORIS, al que se integra el sistema +Firma, concebido como un módulo complementario destinado a la gestión y formalización electrónica de los consentimientos informados de los pacientes.

DOCTORIS constituye el sistema de historia clínica electrónica implantado en los centros del grupo HM, donde se centraliza la recogida, almacenamiento y gestión de los datos personales de los pacientes, incluyendo los datos de salud. Como sistema maestro, DOCTORIS soporta los tratamientos derivados de la asistencia sanitaria y garantiza el cumplimiento de la Ley 41/2002, de autonomía del paciente, así como de los artículos 6 y 9 del Reglamento (UE) 2016/679 (RGPD) en cuanto a legitimación para el tratamiento de categorías especiales de datos.

+Firma, por su parte, es un módulo tecnológico que no realiza recogida directa de datos personales, sino que se nutre de la información previamente introducida en DOCTORIS por HM Hospitales. Su finalidad es permitir la obtención, validación y verificación de la firma electrónica de los documentos relativos al consentimiento informado, aplicando además un sellado de tiempo que asegura la integridad y trazabilidad del acto de firma.

I. *Introducción al sistema +Firma.*

El sistema +Firma es una solución tecnológica implantada en HM Hospitales cuya finalidad exclusiva es facilitar la formalización electrónica de los consentimientos informados de los pacientes, garantizando la autenticidad, integridad y trazabilidad de los documentos firmados.

A diferencia de un sistema autónomo de recogida de datos, +Firma no recaba directamente información de los pacientes, sino que se nutre de los datos ya existentes en el sistema de historia clínica DOCTORIS, que actúa como repositorio principal de la información sanitaria.

El funcionamiento de +Firma se articula en varias fases:

i. *Generación del documento: a partir de plantillas predefinidas de consentimiento informado, previamente elaboradas y validadas por*

HM (Departamento de Calidad y Delegado de Protección de Datos (DPO)), que se completan con los datos del paciente suministrados automáticamente por DOCTORIS.

ii. Captura de la firma: el consentimiento se presenta en tablets dentro de los centros asistenciales, donde el paciente lo visualiza y procede a firmar electrónicamente.

iii. Registro automático: una vez firmado, el sistema genera un documento en formato PDF con sello de tiempo y lo almacena de manera automática en los servidores internos de HM, bajo un esquema de cifrado y encriptación de nombres de archivo.

iv. Uso e integración: el documento firmado queda vinculado a la Historia Clínica Electrónica del paciente en Doctoris, accesible únicamente al personal autorizado en función de sus permisos.

v. Conservación y supresión: los documentos se conservan conforme a los plazos legales de la Ley 41/2002 (mínimo cinco años desde el alta del proceso asistencial) y la normativa autonómica aplicable, aplicándose posteriormente medidas de bloqueo y supresión.

vi. Todo el sistema opera en infraestructura on premise, en servidores bastionados y sin salida a Internet, cumpliendo con las medidas del Esquema Nacional de Seguridad (ENS, categoría alta) y certificaciones internacionales como ISO 27001, ISO 25000 e ISO 33001.

En consecuencia, +Firma debe entenderse como un módulo accesorio de DOCTORIS, diseñado para dar soporte al proceso de consentimiento informado de los pacientes en formato electrónico, sin crear nuevas categorías de datos ni ampliar finalidades de tratamiento." (…)

Con respecto al primer punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación , 1.- Recopilación de datos que lleva a cabo dicho sistema (Categorías de datos y datos recopilados), HMH manifiesta que "*El sistema +Firma no realiza recopilación autónoma de datos personales, en el sentido establecido por el artículo 4.2 del RGPD, que define el tratamiento como "cualquier operación realizada sobre datos personales, como la recogida, registro, organización, conservación, etc.".*

En este caso:

• Los datos personales (identificativos) son previamente recabados por HM Hospitales en el marco de la asistencia sanitaria, con base en la Ley 41/2002, de autonomía del paciente, y se registran en el sistema de historia clínica DOCTORIS.

• +Firma no recaba datos de salud directamente de los pacientes. No existe introducción manual ni recogida activa de información clínica en la aplicación.

• +Firma no añade nuevas operaciones de recogida, sino que se limita a alimentarse de los datos ya existentes en DOCTORIS para incorporarlos en las plantillas de consentimiento informado elaboradas por HM Hospitales.

> *• Por tanto, el sistema no amplía categorías de datos ni introduce finalidades distintas a las que ya justifican la existencia de la historia clínica, de conformidad con los artículos 6.1.c) (obligación legal) y 9.2.h) (tratamiento de datos de salud con fines asistenciales) del RGPD.*

Esta configuración se ajusta al principio de minimización de datos del artículo 5.1.c) RGPD, que exige que los datos personales sean adecuados, pertinentes y limitados a lo necesario para la finalidad del tratamiento." (…)

Con respecto al segundo punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 2.- Base de legitimación para la recogida de esos datos, HMH indica que "*El tratamiento de datos personales vinculado al sistema +Firma encuentra plena cobertura en el marco legal vigente, en tanto que constituye una herramienta accesoria destinada a la formalización electrónica del consentimiento informado de los pacientes, como a la acreditación del cumplimiento del deber de información en materia de protección de datos en el marco de la relación asistencial," (…)* en los artículos 6.1.b) y c) y 9.2.h) del RGPD.

(…) "El sistema +Firma se limita a instrumentar documentalmente un requisito inherente a la prestación de la asistencia sanitaria, sin suponer una finalidad distinta." (…)

Con respecto al tercer punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 3.- Finalidades de la recogida de los datos**,** HMH destaca que *"El sistema +Firma no constituye un tratamiento autónomo, sino un instrumento técnico al servicio de la finalidad legal y asistencial que ya corresponde a la Historia Clínica Electrónica (Doctoris). Las finalidades concretas son las siguientes:*

1. *Formalización del consentimiento informado." (…)*
2. *Acreditación del cumplimiento del deber de información en protección de datos." (…)*
3. *Garantía de autenticidad e integridad del documento. El sistema incorpora firma electrónica y sellado de tiempo." (…)*
4. *Incorporación a la Historia Clínica. Los consentimientos formalizados mediante +Firma se integran en la Historia Clínica Electrónica (DOCTORIS)." (…)*
5. *Trazabilidad y responsabilidad proactiva*." (…)

Con respecto al cuarto punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 4.- Información que la parte reclamada facilita a las personas físicas en el momento de la recogida de datos, HMH manifiesta que: *"La obligación de informar al paciente se articula en un doble plano: el sanitario (Ley 41/2002) y el de protección de datos (RGPD y LOPDGDD*). HM Hospitales cumple con ambos niveles de exigencia en el marco del uso de +Firma.

Así se les suministra Información asistencial en cumplimiento de la Ley 41/2002; e Información en materia de protección de datos (RGPD y LOPDGDD, indicándose que: (…) "*• La información se integra en las plantillas de consentimiento que se ponen a disposición en las tablets, y se facilita igualmente a través de los canales habituales de HM Hospitales (documentación en papel, web corporativa, Portal del Paciente). • En dichas cláusulas se detallan la identidad del responsable, las finalidades del*

tratamiento, los derechos del interesado (acceso, rectificación, supresión, limitación, oposición, portabilidad), el contacto del Delegado de Protección de Datos, así como el acceso a la información adicional en la Política de Privacidad." (…) Y que +Firma supone una transparencia reforzada, ya que (…) *"el sistema +Firma no sustituye el deber de informar, sino que lo instrumentaliza." (…)*

Con respecto al quinto punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 5.-Actividades de tratamiento afectadas por la recogida de los datos, HMH señala que "*La utilización de +Firma se encuentra plenamente integrada en las actividades de tratamiento ya declaradas en el Registro de Actividades de Tratamiento (RAT) de HM Hospitales. No constituye un tratamiento autónomo ni crea nuevas categorías, así como no tiene acceso dentro de estos tratamientos a categorías especiales de datos, sino que se limita a instrumentar la formalización del consentimiento informado dentro de la Historia Clínica Electrónica.*

Concretamente, los tratamientos afectados son:

1. *Historia Clínica Electrónica.*
   o Naturaleza: Mixto.
   o Categoría: Especial.
   o Justificación: los consentimientos firmados mediante +Firma forman parte de la documentación clínica del paciente y se incorporan automáticamente a su HCE, en cumplimiento del art. 17 Ley 41/2002.
2. *Portal del Paciente.*
   o Naturaleza: Digital.
   o Categoría: Especial.
   o Justificación: cuando los consentimientos firmados están disponibles para consulta por parte del paciente a través de este canal digital.
3. *Videoconsulta e Historial Radiológico*
   o Naturaleza: Mixto / Digital.
   o Categoría: Especial.
   o Justificación: determinados consentimientos específicos (telemedicina, pruebas de imagen) pueden formalizarse electrónicamente a través de +Firma."

Con respecto al sexto punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 6.- Análisis de las implicaciones que la recogida de esos datos puede tener en los derechos de protección de datos de las personas, HMH indica que *"La implantación del sistema +Firma no genera riesgos adicionales ni merma los derechos reconocidos a los pacientes en los artículos 15 a 22 del RGPD (derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición). Al contrario, introduce garantías adicionales que refuerzan la posición del interesado" (…) "El uso de firma electrónica y sellado de tiempo añade un valor probatorio que protege tanto al paciente como al centro frente a disputas sobre la validez o integridad del consentimiento. El sistema de cifrado, la limitación de accesos y la conservación on premise en servidores bastionados de HM Hospitales refuerzan la confidencialidad y disponibilidad, principios del art. 5.1.f) RGPD*." (…)

Con respecto al séptimo punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 7.- Medidas de seguridad establecidas para la

garantía de los derechos de las personas físicas en la recopilación de los datos y en su tratamiento posterior, HMH manifiesta que *"En lo que respecta a +Firma desde nuestro lado se adoptan las siguientes medidas de seguridad relativas a protección de datos:*

- (…)

Con respecto al octavo punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 8.- Plazo de conservación de los datos, existencia o no de cesión de los datos a terceros, cesiones internacionales de datos, elaboración de perfiles, HMH señala que: *"Los plazos de conservación de los datos están determinados por el responsable del tratamiento, de conformidad con el art. 17 de la Ley 41/2002" (…) "No obstante, dichos plazos pueden variar en función de la normativa autonómica" (…) "Finalmente, en lo relativo a la elaboración de perfiles, no se llevan a cabo tratamientos automatizados destinados a crear perfiles individualizados de los pacientes. Los datos personales se utilizan exclusivamente para las finalidades asistenciales, administrativas y legales derivadas de la prestación del servicio sanitario."*

Con respecto al noveno punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 9.- Análisis de riesgos, y en su caso, Evaluación de Impacto realizada para llevar a cabo la recopilación de esos datos por dicho sistema, HMH destaca lo siguiente: "*El sistema +Firma ha sido objeto de una Evaluación de Impacto en materia protección de datos (EIPD) realizado por HM Hospitales, en su condición de responsable del tratamiento, contando para ello con el apoyo técnico de sus encargados* ******EMPRESA.2 y ***EMPRESA.3.*** *Su integración en la Historia Clínica Electrónica de HM garantiza que los riesgos identificados se gestionen de forma centralizada y documentada." (…)*

Con respecto al noveno punto del requerimiento practicado, en el marco de las citadas actuaciones previas de investigación, 10.- Participación del DPD en el análisis de riesgos y la evaluación del impacto del sistema (Se deberán aportar los informes del DPD, en su caso), HMH informa que: "*El DPO de HM Hospitales ha desempeñado un papel activo de supervisión, control y asesoría, asegurando que +Firma se utiliza de manera conforme al RGPD, la LOPDGDD y la Ley 41/2002."* (…) *"Con ocasión del presente requerimiento, y en aplicación del artículo 35.11 RGPD, el DPO ha remitido una versión revisada de la EIPD con fecha actualizada, incorporando observaciones recientes y actualizando las medidas de seguridad en función de la evolución tecnológica y organizativa" (…)*

Finalmente, HMH establece como conclusiones finales de su escrito de contestación al requerimiento que:

> *(…) "1. El sistema +Firma no constituye un tratamiento autónomo de datos personales, sino un módulo accesorio integrado en Doctoris, cuya única finalidad es la formalización electrónica de los consentimientos informados exigidos por la Ley 41/2002, así como acreditar el cumplimiento del deber de información previsto en el art. 13 RGPD, con plena cobertura en los artículos 6.1.b), 6.1.c) y 9.2.h) RGPD.*

2. No existe recopilación directa de datos de salud por parte de +Firma. La aplicación se limita a procesar los datos ya incorporados en Doctoris, sin ampliar categorías ni finalidades, en estricto respeto al principio de minimización de datos del artículo 5.1.c) RGPD.
3. Las finalidades del sistema se reducen a: (i) documentar el consentimiento informado; (ii) garantizar la autenticidad e integridad mediante firma electrónica y sello de tiempo; (iii) asegurar su incorporación en la Historia Clínica. No existe ningún uso adicional de los datos.
4. HM Hospitales ha desplegado medidas técnicas y organizativas robustas ***(…),*** *cumpliendo con el artículo 32 RGPD y con el Esquema Nacional de Seguridad.*
5. Se han realizado análisis de riesgos y EIPD lo que demuestra cumplimiento del art. 35 RGPD y del principio de responsabilidad proactiva (art. 5.2 RGPD).
6. La participación del DPO ha sido efectiva y constante en las fases de validación de plantillas, asesoramiento en minimización y conservación, y supervisión de incidentes, cumpliendo lo dispuesto en los arts. 37-39 RGPD y en el art. 34 LOPDGDD.
7. La relación con terceros está limitada y correctamente instrumentada:
- ***o ***EMPRESA.2*** *como encargado (contrato 2019, art. 28 RGPD). Se aporta como Anexo III.*
- *o* ******EMPRESA.3*** *Informática como subencargado técnico, único autorizado. o No existen otros terceros ni transferencias internacionales de datos.*

8. La operativa de +Firma refuerza los derechos de los pacientes (arts. 15 a 22 RGPD), al garantizar trazabilidad y acceso a consentimientos firmados de manera auténtica y segura, sin restricción en el ejercicio de sus derechos.
9. HM Hospitales ha demostrado en todo momento diligencia, transparencia y voluntad de colaboración con la AEPD, manteniendo informados a los pacientes y documentando sus actuaciones conforme a la normativa de protección de datos y sanitaria aplicable." (…)

Adicionalmente, HMH aporta la siguiente documentación:

a) Anexo I, la Cláusula informativa del tratamiento de datos mostrado a los pacientes.

b) Anexo II, EIPD del sistema +Firma de fecha 19 de septiembre de 2025, cuya aprobación consta el 22 de septiembre de 2025.

c) Anexo III. Copia del contrato de encargo de tratamiento. El contrato aportado es el suscrito entre la parte demandada y ******EMPRESA.3***, en fecha 1 de junio de 2019. No es el firmado con la empresa que suministra el servicio ViDSigner.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la LOPDGDD, es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Minimización de datos

La letra c) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:
(…)

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

III
Evaluación de impacto relativa a la protección de datos

El artículo 35.1 del Reglamento (UE) 2016/679 (RGPD) establece la obligación de realizar una evaluación de impacto antes del tratamiento cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías y atendiendo a su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

> *"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares."*

IV
Resultado de las actuaciones de investigación

En el presente caso, la investigación se centra, por un lado, en determinar si con la implementación del sistema de recogida de datos y firma digital, HMH estaría llevando a cabo un tratamiento que implica la recopilación de una cantidad de datos personales excesiva e innecesaria para la finalidad de verificación de la identidad de los destinatarios de la documentación. En particular, si se estarían recabando datos relativos al dispositivo empleado, el identificador IMEI, la geolocalización y otros datos adicionales, cuando sería suficiente, a su juicio, con una mera firma digital para validar la identidad del receptor.

Según se desprende de la información facilitada por HMH

> *"En el marco de la actividad asistencial desarrollada por HM Hospitales, la gestión de la información clínica se articula a través de DOCTORIS, al que se integra el sistema +Firma, concebido como un módulo complementario destinado a la gestión y formalización electrónica de los consentimientos informados de los pacientes.*
>
> *DOCTORIS constituye el sistema de historia clínica electrónica implantado en los centros del grupo HM (…)*

HMH en su respuesta al requerimiento de fecha 24 de septiembre de 2025, afirma que no se amplían categorías de datos tratados, sino que solo trata datos identificativos existentes. Igualmente señala que no se alteran las finalidades originales, sino que el tratamiento se limita a garantizar la formalización electrónica del consentimiento, exigida por la Ley 41/2002, art. 8: (…) "*El sistema +Firma no realiza recopilación autónoma de datos personales, en el sentido establecido por el artículo 4.2 del RGPD, que define el tratamiento como "cualquier operación realizada sobre datos personales, como la recogida, registro, organización, conservación, etc.".*

> *• Los datos personales (identificativos) son previamente recabados por HM Hospitales en el marco de la asistencia sanitaria, con base en la Ley 41/2002, de autonomía del paciente, y se registran en el sistema de historia clínica DOCTORIS.*
> *• +Firma no recaba datos de salud directamente de los pacientes. No existe introducción manual ni recogida activa de información clínica en la aplicación.*
> *• +Firma no añade nuevas operaciones de recogida, sino que se limita a alimentarse de los datos ya existentes en DOCTORIS para incorporarlos en las plantillas de consentimiento informado elaboradas por HM Hospitales.*
> *• Por tanto, el sistema no amplía categorías de datos ni introduce finalidades distintas a las que ya justifican la existencia de la historia clínica, de conformidad con los artículos 6.1.c) (obligación legal) y 9.2.h) (tratamiento de datos de salud con fines asistenciales) del RGPD." (…)*

Explica que "*La utilización de +Firma se encuentra plenamente integrada en las actividades de tratamiento ya declaradas en el Registro de Actividades de Tratamiento (RAT) de HM Hospitales. No constituye un tratamiento autónomo ni crea nuevas categorías, así como no tiene acceso dentro de estos tratamientos a categorías especiales de datos, sino que se limita a instrumentar la formalización del consentimiento informado dentro de la Historia Clínica Electrónica*"

Del análisis de la EIPD y del resto de la documentación obrante en el expediente no consta que se recojan datos innecesarios y excesivos para la finalidad que se persigue. Conviene precisar además que HMH ha manifestado que el proceso de firma electrónica no implica la captación de datos adicionales, sin que exista prueba en contrario.

Asimismo, de las actuaciones se infiere que los datos tratados se utilizan exclusivamente para la gestión y formalización electrónica de los consentimientos informados, dejar constancia del cumplimiento del deber de información, proceder a su incorporación a la historia clínica y garantizar la autenticidad, integridad y trazabilidad de los documentos suscritos, integrándose la solución tecnológica en tres actividades de tratamiento debidamente identificadas, sin que se aprecien indicios de recogida excesiva ni de tratamiento adicional alguno respecto de la finalidad declarada, por lo que no concurren indicios de infracción.

Por otro lado, también se ha comprobado en las actuaciones de investigación que HMH elaboró una Evaluación de Impacto Protección de Datos (EIPD) para el sistema de recolección de datos y firma digital.

Pues bien, HMH realizó una EIPD para el tratamiento de +Firma y así lo refleja en su respuesta al requerimiento de fecha 24 de septiembre de 2025: "*El sistema +Firma ha sido objeto de una Evaluación de Impacto en materia protección de datos (EIPD) realizado por HM Hospitales, en su condición de responsable del tratamiento, contando para ello con el apoyo técnico de sus encargados* ******EMPRESA.2 y ***EMPRESA.3***. *Su integración en la Historia Clínica Electrónica de HM garantiza que los riesgos identificados se gestionen de forma centralizada y documentada." (…)*

En este sentido, consta acreditado que HMH procedió a realizar una EIPD en 2021, procediendo a su actualización en 2025, habiendo sido ambas versiones aportadas a esta Agencia. Si bien la evaluación pudo no elaborarse inicialmente de forma previa al tratamiento, probablemente implantado en junio de 2018, la eventual conducta omisiva cesó en 2021, momento en que se llevó a cabo la elaboración de la EIPD. Dado que el plazo de prescripción comienza a computarse desde el cese de la conducta infractora, la posible infracción del artículo 35 del RGPD por la ausencia de elaboración previa de una EIPD, debe considerarse prescrita, no procediendo la incoación de actuaciones sancionadoras por este extremo.

V Conclusión

El artículo 28.1 de la Ley 40/2015, de Régimen Jurídico del Sector Público señala que "sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa".

En relación con lo anterior, conviene señalar que, al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización, pero

sin excepciones, los principios inspiradores del orden penal, resultando claro la plena virtualidad del principio de presunción de inocencia.

El Tribunal Constitucional en su Sentencia 76/1990, de 26 de abril, en relación con el derecho a la presunción de inocencia y del principio de culpabilidad establece: No puede suscitar ninguna duda que la presunción de inocencia rige sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, sean penales, sean administrativas en general o tributarias en particular, pues el ejercicio del ius puniendi en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el derecho a la presunción de inocencia comporta: que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio."

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que "nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."

Así las cosas, estos principios impiden imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan esta imputación o se conozca con certeza la identidad del presunto infractor, aplicando el principio "in dubio pro reo" en caso de duda.

En este caso, no habiéndose obtenido ni incorporado al procedimiento elementos suficientes que permitan justificar el inicio de un procedimiento sancionador, procede aplicar el principio in dubio pro reo, en conexión con el derecho fundamental a la presunción de inocencia consagrado en el artículo 24.2 de la Constitución Española, plenamente aplicable al ámbito del procedimiento administrativo sancionador, debiendo resolverse el presente expediente en sentido favorable al investigado al no haber quedado desvirtuada su presunción de inocencia.

En consecuencia, procede el archivo de las presentes actuaciones al no haberse obtenido y acreditado una prueba de cargo acreditativa de los hechos de acuerdo con consolidada jurisprudencia del Tribunal Constitucional y Tribunal Supremo (entre otras, la STS Sala 2ª 459/2018 de 10 de octubre).

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a HM HOSPITALES 1989, S.A.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

1245-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos