- **Expediente N.º: EXP202201000 (PS/00626/2022)**

- RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.*** (en adelante, la parte reclamante) con fecha 12 de enero de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA con NIF S4611001A (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que se han realizado accesos indebidos a su historia clínica por cuatro compañeros de trabajo, uno de ellos su superior inmediato. Lo ha puesto en conocimiento del responsable del tratamiento y no ha recibido respuesta.

Junto a la notificación se aporta escrito de representación, solicitud de datos de acceso indebido dirigida a la Unidad de Informática del Hospital de la Fe de la Consejería de Sanidad Universal y Salud Pública de la Generalitat Valenciana, informe emitido por la Subdirección de Sistemas de Información del Hospital La Fe sobre los accesos de los usuarios a parte de las pruebas de la Historia Clínica de la parte reclamante y, por último, queja presentada ante el Sindic de Greuges.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), con fecha de 8 de febrero de 2022 se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 8 de febrero de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 8 de marzo de 2022 se recibe en esta Agencia informe remitido por el Delegado de Protección de Datos de la Generalitat Valenciana con el contenido que consta en el Hecho Probado Sexto.

Con fecha 9 de marzo de 2022, se recibe en esta Agencia un escrito en respuesta al traslado de la reclamación, al que se adjunta una serie de documentos.

TERCERO: Con fecha 12 de abril de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 17 de mayo de 2022, tras analizarse la documentación que obraba en el expediente, se dictó resolución por la Directora de la Agencia Española de Protección de Datos, acordando el archivo de la reclamación. La resolución fue notificada a la parte reclamante con fecha 23 de mayo de 2022, a través del Servicio de
Notificaciones Electrónicas y Dirección Electrónica Habilitada según certificado que figura en el expediente.

QUINTO: Con fecha 21 de junio de 2022, la parte reclamante interpuso un recurso de reposición a través del Registro Electrónico de esta Agencia, contra la resolución recaída en el expediente EXP202201000, por la que se acordaba el archivo de la reclamación. Junto al recurso se aportó nueva documentación relevante a los efectos de lo planteado en la reclamación, concretamente, una serie de correos electrónicos intercambiados con el supervisor de ***PUESTO.3 en el que le informaba de la situación de baja médica ***(...)***; este supervisor había entrado en la historia clínica de la parte reclamante 5 minutos antes de remitirle un correo electrónico solicitando a la parte reclamante información sobre el resultado de sus pruebas, por lo que no accedió a la información de su historia clínica por motivos asistenciales, sino por cuestiones organizativas de los turnos de trabajo.

Con fecha 11 de octubre de 2022**,** la Subdirectora General de Inspección de Datos acordó remitir a la CONSELLERÍA el recurso interpuesto por la parte reclamante, concediéndole trámite de audiencia para formular alegaciones y presentar los documentos y justificantes que estime procedentes, con arreglo a lo dispuesto en el artículo 118 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Notificado el citado trámite de audiencia con fecha 13 de octubre de 2022 conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, el 27 de octubre de 2022 la parte reclamada presentó escrito de alegaciones que se ha incorporado al expediente.

SEXTO: Con fecha 17 de noviembre de 2022 por la Directora de la Agencia Española de Protección de Datos se dictó resolución de recurso de reposición, por la que se estimaba el recurso interpuesto por la parte reclamante y se acordaba admitir a trámite la reclamación formulada de acuerdo con lo establecido en el artículo 65 de la LOPDGDD.

SÉPTIMO: Con fecha 24 de febrero de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, así como por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

OCTAVO: Notificado con fecha 27 de febrero de 2023 a la reclamada el citado acuerdo de inicio conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante,

LPACAP), la parte reclamada presentó escrito de alegaciones con el siguiente contenido:

"*PRIMERA. Falta de notificación de la resolución por la cual se acuerda la estimación del recurso interpuesto por el reclamante.*

La resolución por la que se estima el recurso de reposición instado por la parte reclamante no ha sido notificada a esta Conselleria ni a la Delegación de Protección de Datos de la Generalitat Valenciana. Esta situación genera indefensión al tener esta parte conocimiento del resultado del recurso por la notificación del Acuerdo de inicio de procedimiento sancionador.
Asimismo, estas circunstancias han impedido a esta Conselleria formular el correspondiente recurso contra la citada Resolución, de igual forma desconocemos los motivos y la fundamentación por la cual se estiman los argumentos alegados por el reclamante, limitándose el derecho de defensa de esta parte.

SEGUNDA.- En opinión del Comité Local de Seguridad del Hospital La Fe los hechos reclamados no suponen una brecha de seguridad, atendiendo al hecho de la que en la Historia clínica de la Comunidad Valenciana existen suficientes controles físicos para impedir el acceso del personal ajeno a la asistencia sanitaria, y a los puestos de trabajo informáticos donde se consulta la historia clínica(requiere identificación del usuario y contraseña). En este sentido se pronuncia el Comité en su informe remitido a la Agencia Española de Protección de Datos de fecha 8 de febrero de 2022, de igual forma se respondió a la parte reclamante mediante escrito (registro de salida 07/UFE/2021/21865 de fecha 7 de marzo de 2022) que consta aportado como documento Anexo 4 del citado informe del Comité.

Por tanto, los accesos a los historiales clínicos están restringidos y limitados. Únicamente, el personal sanitario en ejercicio de sus funciones está legitimado para acceder a los datos de salud de los pacientes, tal como establecen los protocolos internos y se recalca en las actuaciones formativas ofrecidas al personal del hospital.

TERCERA.- El hospital considera que ha actuado con diligencia en la protección de los datos de los pacientes y que los protocolos de actuación y actividades formativas son adecuados. La Conselleria ya informó a la AEPD sobre estos extremos en la respuesta al requerimiento efectuado, en el informe remitido a la Agencia Española de Protección de Datos de fecha 8 de febrero de 2022 elaborado por el Comité, lo que tuvo como resultado el archivo de las actuaciones.

No obstante, tanto el hospital como la Conselleria están comprometidos con la mejora continua de sus procedimientos buscando garantizar del mejor modo posible la protección de los derechos de pacientes y ciudadanos. Una de estas actuaciones está siendo la revisión de los procedimientos de identificación del personal y de trazabilidad de sus actuaciones.

CUARTA.- Por todo lo anterior, reiterando lo indicado en las alegaciones presentadas en los escritos anteriores y asumiendo el compromiso de actuar dentro de una dinámica de mejora continua, solicitamos el archivo de las actuaciones al entender que los hechos referidos en la reclamación no son merecedores de sanción."

NOVENO: Con fecha 27 de septiembre de 2023 se formuló propuesta de resolución, proponiendo que por la Directora de la AEPD se sancione a la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA, con NIF S4611001A:

- Por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, con un apercibimiento.

- Por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, con un apercibimiento.

Esta propuesta de resolución, que se notificó a la reclamada conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogida en fecha 27 de septiembre de 2023, como consta en el acuse de recibo que obra en el expediente.

DÉCIMO: Con fecha 11 de octubre de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de la reclamada en el que aduce alegaciones a la propuesta de resolución en el que, en síntesis, manifestaba que la Conselleria de Sanidad establece y aplica controles de seguridad para salvaguardar la confidencialidad e integridad de los datos personales. Además, los accesos al historial clínico están restringidos y limitados. Únicamente, el personal sanitario en ejercicio de sus funciones está legitimado para acceder a los datos de salud de los pacientes, tal como establecen los protocolos internos y se recalca en las actuaciones formativas ofrecidas al personal del hospital. Por último, se alega que el hospital aplica suficientes medidas técnicas y organizativas para preservar la seguridad y la privacidad de sus sistemas de información,

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: Con fecha 29 de abril de 2021, la parte reclamante presentó una queja ante el Síndic de Greuges de la Comunitat Valenciana con el siguiente contenido:

"*Soy DUE en el Servicio de Neurofisiología Clínica del Hospital Universitario y Politécnico de La Fe (Valencia).Tengo sospechas fundadas de que diversas personas de mi Servicio han accedido a mi Historia Clínica de Salud sin mi consentimiento. Debido este motivo, solicite al SAIP del hospital el historial de accesos, recibiéndolo solo con fecha y hora ,cargo que ostenta la persona que accede y servicio al que pertenece, pero en ningún momento me facilitan su nombre y apellidos.*
Sin conocer la identidad de las personas que han realizado dicho acceso sin mi autorización no puedo realizar la denuncia pertinente a la AEPD, ¿Como es posible una actuación tan grave sea defendida protegiendo al infractor por encima de los

derechos del afectado? ¿Como me puede ayudar el Síndic de Greuges a reunir esta información? Espero vuestra respuesta en breve y adjunto informe del SAIP."

SEGUNDO: Con fecha 15 de junio de 2021, la parte reclamante se vuelve a dirigir al Síndic de Greuges de la Comunitat Valenciana, con el siguiente mensaje:

"*Realice una queja ante ustedes el día 29/04/2021, que ustedes admitieron a trámite con número de expediente* ******REFERENCIA.1****.*
Dado que ya ha pasado más de un mes desde que se tramito, rogaria saber cómo está la petición de los nombres que han entrado en mi historia y lo que ha contestado la Conselleria o, me informen si no se los van a facilitar cuales son los organismos a los que debo acudir; ya que a otra de mis compañeras si se lo han facilitado tras reclamarlo."

TERCERO: Con fecha 29 de junio de 2021, desde la Consellería de Sanitat Universal i Salut Pública se envía el siguiente mensaje al Síndic de Greuges de la Comunitat Valenciana:

"*Sr. Síndic:*
Atendiendo a su solicitud de información sobre la queja indicada y su registro de salida ******REFERENCIA.2****, de fecha 03/05/2021, y reiterada en fecha 16/06/2021, se adjunta informe de la Subdirección de Sistemas de Información, de la Gerencia del Departamento de Salud de València-La Fe, con la información solicitada por la promotora de la queja.*

Sirva el presente escrito como respuesta a la notificación recibida.

Damos así cumplimiento a lo establecido en el artículo 19.1 de la Ley 11/1988, de 26 de diciembre, del Síndic de Greuges y las obligaciones contraídas por las administraciones públicas."

CUARTO: Con fecha 7 de junio de 2021 la Subdirección de Sistemas de Información, de la Gerencia del Departamento de Salud de València-La Fe emitió un informe con ocasión de la petición realizada el día 3 de mayo de 2021 por el Síndic de Greuges de la Comunitat Valenciana, con objeto de dar respuesta a la queja interpuesta por la parte reclamante. En dicho informe, remitido el 29 de junio de 2021 desde la Consellería de Sanitat Universal i Salut Pública al Síndic de Greuges de la Comunitat Valenciana, consta lo siguiente:

"*En atención a su solicitud esta Subdirección de Sistemas de Información del Hospital La Fe le remite el "informe de los movimientos informáticos hasta la actualidad de la historia clínica* ******REFERENCIA.3****", con el fin de dar cumplimiento a lo solicitado por* ***Dña. A.A.A.****.*
Habiéndose consultado en la base de datos donde se almacena la información de los accesos de los usuarios a parte de las pruebas de la Historia Clínica de la paciente, se ha obtenido que los usuarios que han accedido a la información clínica disponible en el Hospital La Fe del número de Historia Clínica ******REFERENCIA.3*** *son los que a continuación se detallan:*
Accesos a la historia clínica ******REFERENCIA.3*** *de especializada (ordenados cronológicamente de más a menos reciente):*

Fecha y Hora	Cargo	Servicio	Nombre y Apellidos
28/01/2021 10:42	***PUESTO.1**	NEUMOLOGÍA Y ALEGIA INFANTIL [CEX]	**B.B.B.**
28/01/2021 10:28	***PUESTO.2**	UNIDAD DE ENFERMERIA E50	**C.C.C.**
[…]			
15/07/2020 10:04	***PUESTO.3**	NEUROFISIOLOGIA	**D.D.D.**
[…]			
01/06/2020 13:37	***PUESTO.3**	NEUROFISIOLOGIA	**E.E.E.**

QUINTO: Con fecha 24 de septiembre de 2021 la parte reclamante presenta escrito dirigido al responsable de tratamiento de datos del Departamento de Salud-La Fe, con el siguiente contenido:

"*Que a través de la Subdirección de sistemas de información (escrito de fecha de 7 de junio de 2021) y previo requerimiento del Síndic de Greuges la compareciente ha conocido una serie de intromisiones ilegítimas en su historia clínica nº 643698 efectuadas por **doña E.E.E.** en fecha 1 de junio de 2020, el 15 de julio de 2020 por **doña D.D.D.**, y el 28 de enero de 2021 **por doña B.B.B.** y **don C.C.C.**.*

Que no estando los mismos autorizados para la consulta de su historia clínica en ningún momento por la compareciente, entiendo que se ha producido una intromisión injustificada en mi historia clínica, por lo que se hace necesario que se justifique por el responsable del tratamiento de datos la causa de dicho acceso ilegal, por si existiera alguna brecha de seguridad en el tratamiento de los datos.

Por todo ello,

Solicito del responsable del tratamiento de datos, que se justifique dicho acceso ilegal a mi historia clínica y se investigue si ha existido alguna brecha en la seguridad de dicho tratamiento de datos."

SEXTO: Con fecha 8 de marzo de 2023, en respuesta al traslado de la reclamación a la parte reclamada realizada por esta Agencia, se remite a esta Agencia por el Delegado de Protección de Datos de la Generalitat Valenciana un informe realizado por la Dirección Gerencia del Departamento de Salud Hospital La Fe-Valencia de la Conselleria de Sanidad Universal y Salud Pública, en que se dice que:

"*ANTECEDENTES*

*Que **Doña A.A.A.** había presentado con fecha 24 de septiembre de 2021 escrito dirigido al responsable del tratamiento en el que pedía se aclarase si hubo o no acceso indebido a su Historia Clínica, y se justificase el hecho por el responsable del tratamiento, y se determinase si el acceso suponía una brecha de seguridad.*

*Que **Doña A.A.A.** aportó un informe de accesos proporcionado por la Subdirección de Sistemas de este Hospital, donde se constata que el usuario de puesto de trabajo informático correspondiente a las personas que constan en la reclamación accedieron a su historia clínica en los días indicados.*

Que posteriormente, con fecha 12 de enero de 2022 la interesada ha dirigido Reclamación a la Agencia Española de Protección de Datos, motivando su reclamación en no haber recibido respuesta del responsable del tratamiento a las aclaraciones solicitadas por presuntos accesos indebidos a su Historia Clínica.

*Que de las cuatro personas citadas en la Reclamación hay una, **B.B.B.**, que, según informa la Dirección ***PUESTO.1, no consta en el registro de personal ninguna persona con dicho nombre que haya desempeñado funciones propias del personal dependiente de esta Dirección.*

Que el resto de personas investigadas son personal sanitario en este Hospital, y su puesto de trabajo requiere acceso a la Historia Clínica electrónica de todos los pacientes, con las autorizaciones y restricciones funcionales que marca la normativa al respecto.

Que el personal sanitario ejerce su profesión de acuerdo con su código Deontológico, cuyo conocimiento está en los fundamentos de su formación y es una norma de auto regulación ética aceptada y que inspira y guía su conducta.

Que el Hospital informa a sus empleados, por varios medios, que los accesos a la Historia Clínica del personal que presta servicio en el Hospital se deben realizar estrictamente en el ejercicio de las funciones del puesto que ocupan. Y que cualquier otro acceso debe considerarse un acceso indebido.

RESPUESTA A LA SOLICITUD DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.

Decisión adoptada a propósito de esta reclamación.

Ante la primera petición de la recurrente (de fecha 24/09/21) se trató el tema en reunión del Comité Local de Seguridad de la Información el 6 de octubre de 2021, constando en acta que, "ante la petición de estudio de una brecha de seguridad, se redacta respuesta aclarando que no la hubo y exponiendo las medidas de seguridad técnicas y organizativas aplicadas en el hospital y las averiguaciones que lo constatan".
El Hospital reconoce que, aun habiendo tratado el asunto en el Comité Local de Seguridad de la Información en un tiempo razonable, en el momento de presentarse la reclamación de la interesada ante la Agencia todavía no se había cursado la respuesta, que estaba encolada mientras se atendían otros asuntos. Pero que la respuesta ya está en curso según documentación aportada más adelante.
*Desde la Dirección ***PUESTO.1 se han iniciado averiguaciones con las tres personas trabajadoras del Hospital titulares de los usuarios que afirma la afectada son los autores de los accesos indebidos; a saber, **Doña E.E.E., Doña D.D.D., y Don C.C.C.**.*
Se adjuntan las respuestas obtenidas de los mismos, (Anexos 1, 2 y 3). Se recuerda que de la lista suministrada, hay un nombre que no corresponde a ninguna persona de este Hospital.
*Cabe decir al respecto, sin perjuicio de los resultados que arroje la investigación iniciada sobre los accesos indebidos a la historia de **Doña A.A.A.**, que el citado Comité entiende que no hubo brecha de seguridad, atendiendo al hecho de que en la*

Historia Clínica de la Comunidad Valenciana existen suficientes controles físicos para impedir el acceso de personal ajeno a la asistencia sanitaria, o con intenciones maliciosas, a los puestos de trabajo informáticos que consultan la Historia Clínica Electrónica.
A la vista de los registros de acceso, constatamos que fueron hechos por personal sanitario que cuenta con autorización de acceso en el ejercicio de sus funciones, no habiendo encontrado evidencias de afección a la integridad, o la disponibilidad de la Historia Clínica electrónica objeto de la reclamación.

Acreditación de la respuesta facilitada al reclamante.

Se adjunta documento con la respuesta registrado de salida ***(Anexo 4),*** *en el que se informa a la parte reclamante que se está investigando los accesos indebidos, y que no existe un riesgo de seguridad fuera de los umbrales admitidos por la Conselleria de Sanidad Universal y Salud Pública, por lo que el Comité Local de Seguridad de la Información no clasifica lo reclamado como una brecha de seguridad.*

Causas que han motivado la incidencia que ha originado la reclamación.

La causa principal de esta incidencia es la posibilidad de acceso que tiene el personal asistencial a la Historia Clínica Electrónica del paciente en los hospitales públicos de la Comunidad Valenciana.

Este acceso universal a la Historia Clínica Electrónica se otorga a todos los sanitarios contratados en el sistema de salud de la Comunidad Valenciana en el ejercicio de sus funciones, estando fundado este hecho en el criterio de primar el interés general de preservar la salud individual, mediante el tratamiento ubicuo de cualquier episodio clínico de un ciudadano de la Comunidad Valenciana en los centros asistenciales que gestiona la Conselleria de Sanidad Universal y Salud Pública, y por cualquier profesional formalmente acreditado.

Medidas adoptadas para evitar que se produzcan incidencias similares

Las medidas técnicas y organizativas que garantizan la seguridad en el acceso a la Historia Clínica electrónica de la Comunidad Valenciana, así como las reglas funcionales de los aplicativos que gestionan dicha historia, se definen por la Conselleria de Sanidad Universal y Salud Pública, atendiendo a sus competencias asignadas.

El acceso a la Historia Clínica Electrónica queda restringido a los profesionales sanitarios en función de su rol en el sistema, mediante la aplicación de medidas técnicas y organizativas de acuerdo con el RD 3/2010 que regula el Esquema Nacional de Seguridad. Cualquier otra persona ajena a la prestación asistencial no tiene acceso a los sistemas de información que conforman la Historia Clínica Electrónica.

El Departamento de Salud está especialmente concienciado en su responsabilidad ante la custodia de los datos de sus pacientes, y lleva tiempo aplicando estas medidas.

No obstante, no se puede negar que los profesionales legítimamente habilitados para acceder a la Historia Clínica electrónica pueden incurrir en algún momento, por desconocimiento, error o mala fe, en un acceso indebido a la Historia Clínica electrónica de un paciente.

Para evitar que una persona profesional legítimamente habilitada para el acceso, incurra en un acceso indebido, la Conselleria de Sanidad Universal y de Salud Pública se centra en la formación, información y concienciación de sus personal. Son medidas aplicadas para conseguir la plena formación, concienciación e información de las personas profesionales de este Departamento:

1- *En el acto de entrega y firma del contrato laboral, se incluye la firma de un anexo con información relativa a la protección de los datos a los que accederá en el desempeño de sus funciones.*
2- *Se han desplegado diversos enlaces en el portal de seguridad de la intranet del departamento con información destinada a este propósito formativo.*
3- *El Formulario de Solicitud de Acceso a los Sistemas de Información del Hospital incluye una página dedicada a la normativa de uso de los sistemas, y al deber de secreto en los accesos a la información en el ejercicio de sus funciones. Se adjunta documento (Anexo 5).*
4- *El Hospital programa Planes de Comunicación anuales específicos para cada colectivo. Se adjunta un ejemplo de sesión anual para los nuevos médicos residentes. (Anexo 6)*
5- *La Conselleria de Sanidad Universal y Salud Pública incluye en sus planes de Formación Continua y continuada Formación y Autoformación en Protección de Datos.*

Medidas alineadas con el Esquema Nacional de Seguridad (ENS)

Las Políticas de Seguridad y las normas de acceso a los sistemas de información de la Generalitat Valenciana, aplican también a la Conselleria de Sanidad Universal y de Salud Pública y a este Departamento de Salud, y se recogen respectivamente en el DECRETO 66/2012 del Consell, por el que se establece la política de seguridad de la información de la Generalitat Valenciana,
(https://dogv.gva.es/portal/ficha_disposicion.jsp?sig=004163/2012&L=1)
y en la ORDEN 19/2013, de 3 de diciembre, de la Consellería de Hacienda y Administración Pública, por la que se establecen las normas sobre el uso seguro de medios tecnológicos en la Administración de la Generalitat.
(https://dogv.gva.es/datos/2013/12/10/pdf/2013_11767.pdf).

Basándose en estas normas, este Departamento ha definido su política de seguridad accesible en la web pública
http://www.lafe.san.gva.es/documents/18/d9239b5c-0a27-4b4e-a3618fe2d778d3b6.

La Normativa de uso de los Sistemas de Información del Departamento de Salud está también recogida en un documento propio divulgado suficientemente en su portal de seguridad, accesible desde la intranet del Hospital. Se adjunta documento con las normas (Anexo 7).

En el supuesto de constatarse un acceso indebido a una historia clínica por parte de personal del Hospital, conllevaría la apertura de una información previa que podría derivar en la propuesta de un expediente disciplinario."

SÉPTIMO: Con fecha 9 de marzo de 2023, se recibe escrito en esta Agencia de la Delegación de Protección de Datos de la Generalitat Valenciana en el que se adjunta la siguiente documentación:

1- Alegaciones ***D.D.D.***, donde se dice lo siguiente:

"*[…] No haber entrado en ningún momento en la historia clínica de la persona denunciante el día 15/07/2020 a las 10:04h como se me ha informado. Como sistemática de trabajo, y tras el poco tiempo que llevaba trabajando en el servicio, ya que mi incorporación fue el día 23/03/2020 en plena pandemia por covid, donde enseguida se me trasladó a otro servicio a ayudar, en las fechas indicadas de la denuncia, habían muchas cosas en las que consultaba dudas de registros y citaciones en los ordenadores, las sesiones clínicas se dejaban abiertas en las distintas partes del servicio de neurofisiología como práctica habitual, por lo que pudo haber accedido entonces cualquier persona desde mi sesión clínica, añadiendo además que apenas había tenido relación en el servicio por el poco tiempo que llevaba en él*." (el subrayado es nuestro).

2- Alegaciones ***E.E.E.****, donde se dice lo siguiente:*
"[…] En esta parte se considera relevante que (…) teníamos iniciada la sesión en el ordenador, con frecuencia debíamos atender los requerimientos propios del servicio, a petición tanto de los pacientes como de los propios médicos, siendo esta situación la responsable de que durante el transcurso de dicho tiempo, los ordenadores quedarán solos y con las sesiones abiertas y otras compañeras puedan hacer uso del ordenador sin cerrar la sesión e iniciar una nueva, continuando con el mismo usuario que se encontraba activo en tal momento, hecho que resulta ser una práctica habitual y cuya finalidad era lograr una mayor optimización de los recursos disponibles." (el subrayado es nuestro).

3- Alegaciones ***C.C.C.***
"[…] Es práctica habitual abrir una o varias sesiones clínicas durante la jornada laboral, que debido a la dinámica de trabajo pueden quedar sin custodia de forma puntual, motivo por el cual y ante la sospecha de que alguien pudiese utilizar mi sesión de forma fraudulenta, solicité el 22 de marzo de 2021 al servicio de informática se bloqueara mi sesión de forma automática a los cinco minutos de inactividad". (el subrayado es nuestro).

4- Carta Respuesta Reclamante ***A.A.A.***
Remitida con fecha 7 de marzo de 2023 desde la Dirección de ***PUESTO.3 del Departamento de Salud del Hospital de la Fe se remite respuesta (página 157 del expediente) a la reclamación interpuesta por la parte reclamante cuyos términos se recogen en el Hecho Probado Quinto. En esta respuesta se dice que:

"Ante las alegaciones de la recurrente, se trató el tema en reunión del Comité Local de Seguridad de la Información el 6 de octubre de 2021, constando en acta al respecto

que, "ante la petición de estudio de una brecha de seguridad, se redacta respuesta aclarando que no la hubo y exponiendo las medidas de seguridad técnicas y organizativas aplicadas en el hospital y las averiguaciones que lo constatan…".

5- Plantilla Solicitud accesos a Sistemas. Se trata de un Formulario de Solicitud de Acceso a los Sistemas de Información del Hospital incluye una página dedicada a la normativa de uso de los sistemas, y al deber de secreto en los accesos a la información en el ejercicio de sus funciones

6- Curso concienciación. Se adjuntan una serie de imágenes del contenido de una sesión formativa que, según la reclamada, se imparte a los nuevos médicos residentes.

7- Normas de uso de los sistemas.
En este documento se dice lo siguiente:

"***1.*** *OBJETIVO*
El objetivo de este documento es establecer las normas de uso del ordenador asignado al puesto de trabajo del personal del DEPARTAMENTO DE SALUD VALENCIA-LA FE, la red corporativa, equipos portátiles, aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, en soporte informático y en soporte papel.

Es fundamental que todos los empleados de DEPARTAMENTO DE SALUD VALENCIA LA FE, que utilizan equipamiento informático y accedan o traten información crítica y de carácter personal para la realización de sus funciones y tareas sean conocedores de esta norma.

2. ALCANCE
Este documento se aplica a todas las actividades del DEPARTAMENTO DE SALUD VALENCIA - LA FE en el ámbito de la obtención, tratamiento y cesión de datos de carácter personal y en el tratamiento de la información esencial. Este Documento es de obligado cumplimiento para todo el personal del DEPARTAMENTO DE SALUD VALENCIA - LA FE o personal externo que tenga acceso a los datos de carácter personal que son tratados por el DEPARTAMENTO DE SALUD VALENCIA - LA FE y a la información de carácter esencial, por lo que se ubicará en el directorio compartido correspondiente, a nivel interno, y será enviada al personal externo por email.

Las presentes normas de seguridad son de aplicación a los recursos protegidos que dispone el DEPARTAMENTO DE SALUD VALENCIA - LA FE. Así como todos aquellos terceros que tratan datos en nombre del DEPARTAMENTO DE SALUD VALENCIA - LA FE.
[…]
4. DESARROLLO
[…]
Los Usuarios deben cumplir con las siguientes medidas de seguridad para el uso de los ordenadores personales:
[…]

• Los equipos portátiles y otros soportes informáticos, única y exclusivamente están a disposición con la finalidad de permitir el desempeño de las funciones y tareas encomendadas, estando prohibido el uso para otras finalidades de carácter personal.

• Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por DEPARTAMENTO DE SALUD VALENCIA - LA FE, son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. De este modo, está prohibido, entre otros: i) emplear identificadores y contraseñas de otros Usuarios para acceder al sistema y a la red de DEPARTAMENTO DE SALUD VALENCIA - LA FE, ii) Intentar modificar o acceder al registro de accesos. iii) Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros y iv) En general, el empleo de la red corporativa, sistemas, equipos informáticos y cualquier medio puesto al alcance del Usuario, vulnerando el derecho de terceros, los propios de este Organismo, o bien para la realización de actos que pudieran ser considerados ilícitos.
[…]
En relación con lo anterior, deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de este Organismo y dispuesto a razón única de las funciones o tareas desempeñadas en DEPARTAMENTO DE SALUD VALENCIA - LA FE, Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el Usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente."

OCTAVO: Con ocasión de la presentación de un recurso de reposición contra el archivo de su reclamación, la parte reclamante presenta una serie de correos electrónicos, con los siguientes datos:

1.- Con fecha 21 de enero de 2021 a las 15:50 horas, desde el correo electrónico ******EMAIL.1*** se envía un correo con el asunto "******ASUNTO.1***", a los siguientes destinatarios: ******EMAIL.2***; ******EMAIL.3***; ******EMAIL.4***. A continuación, se transcribe el mensaje enviado:

"*Informar que el resultado de la PCR de mi hijo ha sido positivo.*
Ya he informado a riesgos laborales para que me den las directrices a seguir.
Atentamente, un saludo

A.A.A."

2.- Desde el correo ******EMAIL.1*** se envió el siguiente mensaje:

"El resultado de la pcr realizada el día 25 ha sido negativa, quedo a expensas del resultado de la pcr que van a realizarme el día 27 para el alta.

Atentamente, ***A.A.A.****"*

3.- Con fecha 28 de enero de 2021 a las 10:33, desde el correo ***EMAIL.3** se envía un correo con el asunto "***ASUNTO.2**" a los siguientes destinatarios: ***EMAIL.2**; ***EMAIL.5**; ***EMAIL.4.** A continuación, se transcribe el mensaje enviado:

"*te hicieron ayer la PCR???*

Como te ha salido???

Te han dado el alta???

Mañana viernes 28 trabajarás??"

4.- Con fecha 28 de enero de 2021 a las 10:46 horas, desde el correo electrónico ***EMAIL.1** se envía un correo con el asunto "***ASUNTO.1**", a los siguientes destinatarios: ***EMAIL.2** y ***EMAIL.3**. A continuación, se transcribe el mensaje enviado:

"*Me acaban de llamar de sprl que el resultado es negativo, así que tendré el alta con fecha de hoy*
A.A.A."

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora 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
Contestación a las alegaciones aducidas al acuerdo de inicio y a las alegaciones aducidas a la propuesta de resolución

A) En relación con las alegaciones aducidas al acuerdo de inicio del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por la parte reclamada en su escrito:

"PRIMERA. Falta de notificación de la resolución por la cual se acuerda la estimación del recurso interpuesto por el reclamante."

La parte reclamada ha tenido la posibilidad de presentar alegaciones respecto a los motivos que llevaron a la estimación del recurso una vez notificado el acuerdo de inicio, en el que se concede un plazo para presentar alegaciones, que son contestadas en este documento, por lo que no se ha producido indefensión.

En cuanto al desconocimiento que alega la parte reclamada de "*los motivos y la fundamentación por la cual se estiman los argumentos alegados por el reclamante"*, la resolución del recurso se incorporó al expediente, por lo que, de acuerdo con lo establecido en el artículo 53.1.a) de la LPACAP, tiene derecho a acceder y a obtener copia de dicha resolución del recurso.

Por todo lo expuesto, se desestima la presente alegación.
"SEGUNDA. En opinión del Comité Local de Seguridad del Hospital La Fe los hechos reclamados no suponen una brecha de seguridad"

Según la parte reclamada "*existen suficientes controles físicos para impedir el acceso del personal ajeno a la asistencia sanitaria, y a los puestos de trabajo informáticos donde se consulta la historia clínica (requiere identificación del usuario y contraseña) … Por tanto, los accesos a los historiales clínicos están restringidos y limitados. Únicamente, el personal sanitario en ejercicio de sus funciones está legitimado para acceder a los datos de salud de los pacientes"*

Sin embargo, en el "informe de los movimientos informáticos hasta la actualidad de la historia clínica ******REFERENCIA.3***" emitido por la Subdirección de Sistemas de Información, de la Gerencia del Departamento de Salud de València-La Fe reproducido en el Hecho Probado Cuarto, consta consulta efectuada fecha 28/01/2021 a las 10:28, por el cargo "supervisor de ***PUESTO.3" ***C.C.C.***, quien cinco minutos más tarde, a las 10:33 de ese mismo día, preguntó por correo electrónico (Hecho Probado Octavo, correo 3) a la parte reclamante si le habían dado el alta y si iba a trabajar ese mismo día. En un correo anterior la parte reclamante había informado a este supervisor que estaba pendiente de una PCR a realizar el día 27 de enero para saber si tendría el alta. Incluso el día 28/01/2021 a las 10:42 horas, con posterioridad a los hechos relatados anteriormente, se produjo el acceso a la Historia Clínica de la parte reclamante por ***B.B.B.***, de quien la reclamada declara que, tal y como se recoge en el Hecho Probado Sexto, "*no consta en el registro de personal ninguna persona con dicho nombre que haya desempeñado funciones propias del personal dependiente de esta Dirección"*. Además, en el informe de la historia clínica ******REFERENCIA.3*** consta dos accesos reflejados de fechas anteriores a los expuestos anteriormente y que tampoco estarían autorizados, al no estar vinculados con algún tratamiento recibido por la parte reclamante en el DEPARTAMENTO DE SALUD DE VALENCIA – LA FE. Por todo ello, por un lado, queda acreditado el acceso indebido de personal del DEPARTAMENTO DE SALUD VALENCIA - LA FE a la Historia Clínica de la parte reclamante, sin que estos accesos estén vinculados a algún tipo de tratamiento que

estuviera recibiendo la parte reclamante en el DEPARTAMENTO DE SALUD VALENCIA - LA FE, y por otro, el acceso a la Historia Clínica de la parte reclamante por un tercero ajeno a la citada organización, que no consta como empleado del servicio en cuestión.

Por todo lo expuesto, se desestima la presente alegación.

"TERCERA.- El hospital considera que ha actuado con diligencia en la protección de los datos de los pacientes y que los protocolos de actuación y actividades formativas son adecuados."

En respuesta a esta alegación cabe señalar que, tanto por los hechos objeto del presente procedimiento como de la documentación remitida por la Delegación de Protección de Datos de la Generalitat Valenciana, se ha puesto de manifiesto la falta de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para evitar los accesos indebidos a la Historia Clínica Electrónica de los pacientes del servicio de salud valenciano. Además, en el propio testimonio de las personas que accedieron de forma injustificada a la Historia Clínica de la parte reclamante se declara que es práctica habitual que las sesiones en los ordenadores queden abiertas y sin custodia (Hecho Probado Séptimo, documentos 1, 2 y 3). En el documento 7 del Hecho Probado Séptimo "Norma de uso de los sistemas", en el que se establece las normas de uso del ordenador asignado al puesto de trabajo del personal del DEPARTAMENTO DE SALUD VALENCIA-LA FE, la red corporativa, equipos portátiles, aplicaciones informáticas se dice que "*Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por DEPARTAMENTO DE SALUD VALENCIA - LA FE, son personales e intransferibles… De este modo, está prohibido, entre otros: i) emplear identificadores y contraseñas de otros Usuarios para acceder al sistema y a la red de DEPARTAMENTO DE SALUD VALENCIA - LA FE*". Sin embargo, que las sesiones de la aplicación de consulta del Historia Clínica pueden quedar abiertas sin bloqueo de sesión automático por inactividad del usuario, pueden permitir que se realicen consultas indebidas a la Historia Clínica por otros usuarios. En una de las declaraciones remitidas por la reclamada, uno de los empleados del DEPARTAMENTO DE SALUD VALENCIA - LA FE solicita al servicio de informática una medida como es el bloqueo de sesión automático a los cinco minutos de actividad (Hecho Probado Séptimo, documento 3).

Además, las consultas de la Historia Clínica de un paciente deben estar vinculadas a un tratamiento o consulta médica. A modo de ejemplo, debe considerarse un acceso indebido a la Historia Clínica cuando el motivo del mismo es conocer el resultado de una prueba médica a efectos de saber si un compañero va a acudir a trabajar. No puede afirmarse, como hizo el Comité Local de Seguridad de la Información en la respuesta enviada a la parte reclamante (documento 4 del Hecho Probado Séptimo), que no hubo brecha de seguridad y que las medidas técnicas y organizativas aplicadas en el hospital y las averiguaciones lo constatan, siendo justamente lo contrario.

Refiere la CONSELLERÍA que "*Únicamente, el personal sanitario en ejercicio de sus funciones está legitimado para acceder a los datos de salud de los pacientes, tal como establecen los protocolos internos y se recalca en las actuaciones formativas ofrecidas al personal del hospital*", a lo que cabe responder que la brecha de seguridad también

se produce cuando el personal sanitario dependiente de la CONSELLERÍA, aun tratándose de personal interno, realiza un acceso no autorizado a datos de los pacientes, lo que supone una vulneración de lo dispuesto en el artículo 32 del RGPD.

Por otra parte, en respuesta al traslado de la reclamación efectuado por esta Agencia, la CONSELLERIA señala que las medidas adoptadas "*se centra en la formación, información y concienciación de su personal*. Por lo tanto, no se ha justificado ninguna medida específica de carácter técnico u organizativo destinada a evitar el acceso indebido a la Historia Clínica Electrónica de personas que ni siquiera están siendo atendidos por el servicio de salud valenciano; no se ha hecho un análisis de los errores que se han producido y las medidas específicas que podrían evitarlos.

Por todo lo expuesto, se desestima la presente alegación.

B) En relación con las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas según el orden expuesto por la CONSELLERÍA DE SANIDAD:

"*PRIMERA. -Respecto a la calificación de los hechos que suponen una infracción del artículo 5.1.f) del RGPD, con propuesta de una sanción apercibimiento:*"

En esta alegación la reclamada argumenta que, en procedimientos anteriores abiertos por esta Agencia por accesos indebidos a información clínica, no se ha cuestionado la idoneidad ni la suficiencia de dichos controles.

A lo que la parte reclamada se refiere como "*procedimientos anteriores*" no son sino actuaciones de remisión previstas en el artículo 65.4 de la LOPDGDD, a efectos de determinar la admisión o inadmisión a trámite de la reclamación, por lo que no se trata de ningún tipo de procedimiento anterior que haya establecido algún tipo de precedente. Además, la resolución de archivo a que se refiere la reclamada fue revocada mediante resolución de estimación del recurso de interposición interpuesto por la parte reclamante, tal y como se explica en el Antecedente Sexto, debido a que, de la documentación aportada por la parte reclamante, se pudieron apreciar indicios de accesos indebidos, no justificados a su historia clínica electrónica. En la resolución del recurso se declaraba la admisión a trámite de la reclamación, dando lugar a la incoación del presente procedimiento.

Por todo lo expuesto, se desestima la presente alegación.

"SEGUNDA. Respecto a la calificación de los hechos que suponen una infracción del artículo 32 RGPD relacionados con la seguridad del tratamiento:"

En estas alegaciones, la reclamada enumera una serie de medidas técnicas y organizativas para preservar la seguridad y la privacidad de sus sistemas de información.

Concretamente, se recoge una medida para el control del motivo de acceso a las Historias clínicas en la respuesta trasladada por el Hospital La Fe – Valencia a la

CONSELLERÍA, en la que se dice que "*En relación con el riesgo de acceso indebido a la información, concretamos evidencia que respaldan los controles aplicados para prevenirlos:*
[…]
8- Existe en la pantalla de consulta de Historias clínicas, ventana previa su acceso conteniendo un aviso y registrando el motivo por parte del usuario. Se aporta Prueba #8"

Mediante la aplicación de esta medida de control, la reclamada debería poder justificar el motivo por el cual se produjeron los accesos a la Historia Clínica Electrónica de la parte reclamante. Sin embargo, el motivo esgrimido por la reclamada según el cual se produjeron los accesos objeto de la reclamación es el siguiente: "…*No obstante, durante la pandemia de COVID es posible que se realizaran actuaciones puntuales de carácter extraordinario referidas a la ordenación de turnos y organización de las plantillas con objeto de facilitar la atención a los pacientes habida cuenta del incremento de bajas entre el personal sanitario víctima también de la pandemia."*

Pues bien, este argumento se contradice con las declaraciones efectuadas por tres de las personas que accedieron indebidamente a los datos personales de la parte reclamante, reproducidas parcialmente en el Hecho Probado Séptimo.

En el documento "1.- Alegaciones ***D.D.D."*** se afirma "… *No haber entrado en ningún momento en la historia clínica de la persona denunciante"*. En el documento "2- Alegaciones ***E.E.E.***" obrante en el expediente se declara "*que no realicé los accesos que se me imputan*". Del mismo modo, en el documento "3- Alegaciones ***C.C.C.***" obrante en el expediente se declara "*que ni en la fecha señalada en su escrito ni en ninguna otra he accedido a la historia clínica de la ***PUESTO.1…*".

En consecuencia, ninguno de los testimonios de las personas que accedieron indebidamente a los datos de la parte reclamante, puede justificar el argumento de la reclamada, en cuanto a que la causa del acceso haya sido la ordenación de turnos y organización de las plantillas, como defiende la reclamada en su escrito de alegaciones.

Por todo lo expuesto, se desestima la presente alegación.

"TERCERA. - En consecuencia, consideramos que los hechos manifestados en la reclamación no acreditan un comportamiento inadecuado o negligente por parte de esta Conselleria que justifique la sanción propuesta. Independientemente de lo anterior, tanto la Conselleria como la dirección del hospital están comprometidos con la mejora continua de sus procedimientos, buscando garantizar del mejor modo posible la protección de los derechos de pacientes y ciudadanos. En este sentido, una de las actuaciones previstas a raíz de la presente reclamación es la revisión de los procedimientos de identificación del personal, de control de accesos a la información y de trazabilidad de sus actuaciones, así como de los correspondientes refuerzos formativos del personal con acceso a información sensible."

En respuesta a esta alegación, en cuanto al comportamiento atribuible a la reclamada se debe distinguir entre la infracción del artículo 5.1.f) del RGPD y del artículo 32 del RGPD:

a) Infracción del artículo 5.1.f) del RGPD.

De los hechos acreditados en el presente procedimiento se determina la vulneración de la confidencialidad de los datos personales de la parte reclamante, llevada a cabo por personal sanitario dependiente de la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA al consultar, sin motivo que tenga amparo normativo, la Historia Clínica Electrónica de la parte reclamante, lo que determina la responsabilidad administrativa de la citada CONSELLERÍA. A efectos de confirmar la responsabilidad de la CONSELLERÍA de los actos realizados por su personal, cabe traer a colación la Sentencia del Tribunal Supremo núm. 188/2022 (Sala de lo Contencioso, Sección 3ª), de 15 de febrero de 2022 (rec. 7359/2020), cuyo Fundamento de Derecho Cuarto dispone: "*…Como ya sostuvimos en la STS nº 196/2020, de 15 de febrero de 2021 (rec. 1916/2020) el encargado del tratamiento responde también por la actuación de sus empleados y no puede excusarse en su actuación diligente, separadamente de la actuación de sus empleados, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las medidas de seguridad existentes la que fundamenta la responsabilidad de la empresa en el ámbito sancionador por actos "propios" de sus empleados o cargos, no de terceros."*

b) Infracción del artículo 32 del RGPD.

En cuanto a los hechos constitutivos de la infracción del artículo 32 del RGPD atribuibles a la CONSELLERÍA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA, si bien por la reclamada se justifican una serie de medidas técnicas y organizativas para preservar la seguridad y la privacidad de sus sistemas de información, estas medidas no eran las adecuadas para evitar los hechos objeto de reclamación, por lo que la infracción del artículo 32 del RGPD se produce al no existir medidas que evitasen la vulneración producida.

Por todo lo expuesto, se desestima la presente alegación.

III
Integridad y confidencialidad

El artículo 5.1.f) "Principios relativos al tratamiento" del RGPD establece:

"*1. Los datos personales serán:*
(…)
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

En el presente caso, queda acreditado que se ha producido un acceso no autorizado a la historia clínica de la parte reclamante, obrante en la base de datos de la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT

VALENCIANA, vulnerándose el principio de confidencialidad. Según los informes aportados por la parte reclamante, cuatro de los accesos a su historia clínica fueron realizados por personal sanitario (…) pero en ningún caso por motivos asistenciales o sanitarios, (…). El acceso a la historia clínica se produjo por motivos de regulación de los turnos de trabajo, tal y como se desprende de los correos electrónicos aportados por la parte reclamante. En la página 1 del "*informe de los movimientos informáticos hasta la actualidad de la historia clínica* ******REFERENCIA.3***", consta consulta efectuada fecha 28/01/2021 a las 10:28, por el cargo "supervisor de ***PUESTO.3" ***C.C.C.***, quien a las 10:33 de ese mismo día preguntó por correo electrónico a la parte reclamante si le habían dado el alta y si iba a trabajar ese mismo día. En un correo anterior la parte reclamante había informado a este supervisor que estaba pendiente de una PCR a realizar el día 27 de enero para saber si tendría el alta. El día 28/01/2021, con posterioridad a los hechos relatados anteriormente, vuelve a producirse un acceso no autorizado por alguien que no consta en el registro de personal del HOSPITAL LA FE – VALENCIA, según la contestación remitida el 08/03/2022 por la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA en respuesta al traslado de la reclamación efectuado por esta Agencia. Además, la parte reclamante hace referencia a otros dos accesos reflejados en el "informe de los movimientos informáticos hasta la actualidad de la historia clínica ******REFERENCIA.3***" de fechas anteriores a los expuestos anteriormente y que tampoco estarían autorizados.

En este momento procedimental de resolución del procedimiento sancionador, existen evidencias de que se ha vulnerado el artículo 5.1.f) del RGPD, ya que terceros no autorizados tuvieron acceso a los datos personales de la parte reclamante, por lo que no se garantizó su confidencialidad.

IV
Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

De conformidad con las evidencias de las que se dispone en el presente momento de resolución del procedimiento sancionador, se considera que la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA no garantizó debidamente la confidencialidad e integridad de los datos personales de su titularidad.

Los hechos conocidos son constitutivos de una infracción, imputable a la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA**,** tipificada en el artículo 83.5 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

A este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 72 de la LOPDGDD, que califica de muy grave la siguiente conducta:

"*1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"

V

Sanción por la infracción del artículo 5.1.f) del RGPD

El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

"*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."*

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*" de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) …
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d)…

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

Por tanto, por la citada infracción del artículo 5.1.f) del RGPD, corresponde sancionar con apercibimiento a la parte reclamada.

VI
Seguridad del tratamiento

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

> *a) la seudonimización y el cifrado de datos personales;*
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datospersonales de forma rápida en caso de incidente físico o técnico;*
> *d) un proceso de verificación, evaluación y valoración regulares de la eficaciade las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

En el presente caso, tal y como expresa la parte reclamada en su respuesta al traslado de la reclamación efectuado por esta Agencia, la brecha de seguridad se ha producido debido al acceso universal a la Historia Clínica Electrónica, el cual se otorga a todos los sanitarios contratados en el sistema de salud de la Comunidad Valenciana en el ejercicio de sus funciones, por lo que no existen medidas técnicas u organizativas apropiadas que garanticen que no se produzcan accesos indebidos por parte del personal sanitario al servicio de la CONSELLERIA a la consulta de los datos personales existentes en la Historia Clínica Electrónica de los pacientes. En respuesta al traslado de la reclamación efectuado por esta Agencia, la CONSELLERIA señala que las medidas adoptadas "*se centra en la formación, información y concienciación de su personal*". Por lo tanto, no se ha justificado ninguna medida específica de carácter técnico u organizativo destinada a evitar el acceso indebido a la Historia Clínica Electrónica de personas que ni siquiera están siendo atendidos por el servicio de salud valenciano; no se ha hecho un análisis de los errores que se han producido y las medidas específicas que podrían evitarlos. En definitiva, no se justifica la suficiencia de tales medidas para evitar brechas de seguridad similares en el futuro.

En este momento procedimental de resolución del procedimiento sancionador, existen evidencias de que se ha vulnerado el artículo 32 del RGPD, debido a la carencia de medidas apropiadas en función del riesgo para evitar accesos no autorizados.

VII
Tipificación y calificación de la infracción del artículo 32 del RGPD

De conformidad con las evidencias de las que se dispone en el presente momento de resolución procedimiento sancionador, se considera que la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA no cuenta con las medidas apropiadas en función del riesgo para evitar accesos no autorizados como el ocurrido en este caso, teniendo en cuenta, además, que los datos relativos a la salud están incluidos en el artículo 9 del RGPD en las categorías especiales de datos personales, cuyo tratamiento merece mayor protección.

Los hechos conocidos son constitutivos de una infracción, imputable a la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA**,** tipificada en el artículo 83.4 del RGPD, que estipula lo siguiente:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:
a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71 *"Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los dos años, conforme al artículo 73.f) de la LOPDGDD, que califica de grave la siguiente conducta:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes: (…)

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.
(…)

VIII
Sanción por la infracción del artículo 32 del RGPD

El artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD en su apartado 7 establece:

"*Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."*

Asimismo, el artículo 77, "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*", de la LOPDGDD dispone lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) …
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d)…

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.
Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo."

Por tanto, por la citada infracción del artículo 32 del RGPD, corresponde sancionar con un apercibimiento a la parte reclamada

IX
Adopción de medidas

Se acuerda imponer al responsable que en el plazo de 9 meses proceda a adoptar las medidas técnicas y organizativas necesarias para evitar el acceso no autorizado a la Historia Clínica electrónica de los usuarios de los servicios sanitarios prestados por la CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…*". La imposición de esta medida es compatible con la sanción consistente en sancionar con apercibimiento, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA**, con NIF **S4611001A**:

- Por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

- Por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de apercibimiento.

SEGUNDO: ORDENAR a **CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA**, con NIF **S4611001A**, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 9 meses, acredite haber procedido al cumplimiento de medidas técnicas y organizativas necesarias para evitar el acceso no autorizado a la Historia Clínica electrónica de los usuarios de sus servicios sanitarios.

TERCERO: PROPONER a **CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA**, con NIF **S4611001A,** en virtud de lo dispuesto en el artículo 77.3 de la LOPDGDD, la iniciación de actuaciones disciplinarias contra las personas responsables de los accesos indebidos.

CUARTO: NOTIFICAR la presente resolución a **CONSELLERIA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA**.

QUINTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-250923

Mar España Martí
Directora de la Agencia Española de Protección de Datos