

Nota de campo

La evaluación de impacto en protección de datos en los proyectos de investigación



Francisco Javier García-León^{a,b,*}, Román Villegas-Portero^a, Juan Antonio Goicoechea-Salazar^a, Dolores Muñoz-Muñoz^a y Joaquín Dopazo^c

^a Subdirección Técnica Asesora de Gestión de la Información, Servicio Andaluz de Salud, Sevilla, España

^b Grupo de Investigación «Ciencia, Tecnología, Sociedad y Racionalidad Práctica», Facultad de Filosofía, Universidad de Sevilla, Sevilla, España

^c Área de Bioinformática Clínica, Fundación Progreso y Salud, Sevilla, España

INFORMACIÓN DEL ARTÍCULO

Historia del artículo:

Recibido el 12 de septiembre de 2019

Aceptado el 10 de octubre de 2019

On-line el 21 de enero de 2020

Palabras clave:

Protección de datos

Reglamento General de Protección de Datos

Investigación

Keywords:

Data protection

General Data Protection Regulation

Research

R E S U M E N

Los recientes cambios en la normativa europea de protección de datos de carácter personal siguen permitiendo el uso de los datos sanitarios con fines de investigación, pero establecen la evaluación de impacto en protección de datos como instrumento de reflexión y análisis de riesgos en el proceso de tratamiento de datos. La publicación de una guía facilita la realización de esta evaluación de impacto, aunque no es de aplicación directa para los proyectos de investigación. Se detalla la experiencia en un proyecto concreto, y se muestra cómo el contexto del tratamiento toma relevancia respecto a las características de los datos. La realización de una evaluación de impacto es una oportunidad para asegurar el cumplimiento de los principios de la protección de datos en un entorno cada vez más complejo y con mayores desafíos éticos.

© 2019 SESPAS. Publicado por Elsevier España, S.L.U. Este es un artículo Open Access bajo la licencia CC BY-NC-ND (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Impact assessment on data protection in research projects

A B S T R A C T

Recent changes in European regulations for personal data protection still allow the use of health data for research purposes, but they have set the Impact Assessment on Data Protection as an instrument for reflection and risk analysis in the process of data processing. The publication of a guide facilitates this impact assessment, although it is not directly applicable to research projects. Experience in a specific project is detailed, showing how the context of the treatment becomes relevant with respect to the data characteristics. Carrying out an impact assessment is an opportunity to ensure compliance with the principles of data protection in an increasingly complex environment with greater ethical challenges.

© 2019 SESPAS. Published by Elsevier España, S.L.U. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Introducción

El Reglamento General de Protección de Datos¹ (RGPD) establece un marco común para el tratamiento de datos de carácter personal en el ámbito europeo, y la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales² (LOPDGDD), por su parte, desarrolla algunos aspectos instrumentales, pero sin modificaciones ni interpretaciones sobre lo establecido en el RGPD³. Desde la perspectiva de la investigación sanitaria a partir de bases de datos, no se introducen modificaciones sustanciales en cuanto a la posibilidad de tratar estos datos⁴ y se permite el uso secundario de los datos de salud en investigación, pero con unos principios y unos requisitos definidos.

El Artículo 35 del RGPD establece que ante la probabilidad de que un tratamiento «entrañe un alto riesgo para los derechos y libertades de las personas físicas» (esto incluye el tratamiento de datos de

salud) será necesario llevar a cabo una evaluación de impacto en protección de datos (EIPD). Su realización corresponde al responsable del tratamiento de datos (en los proyectos de investigación, el investigador principal), que contará con el asesoramiento del delegado de protección de datos de la institución donde se realice la investigación.

Para ayudar a la realización de la EIPD, la Agencia Española de Protección de Datos (AEPD) ha desarrollado una herramienta para hacer análisis de riesgos y evaluaciones de impacto en la protección de datos⁵, y ha publicado la *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*⁶.

El objetivo de esta nota de campo es comunicar la experiencia del uso de dicha guía en la realización de una EIPD ligada a un proyecto de investigación, y que sirva como ayuda a futuros investigadores que tengan que utilizarla.

Desarrollo de la experiencia

Se realizó una EIPD para el tratamiento de datos en un proyecto de investigación que utilizaba la Base Poblacional de Salud⁷ para

* Autor para correspondencia.

Correo electrónico: fjavier.garcia.leon@juntadeandalucia.es (F.J. García-León).

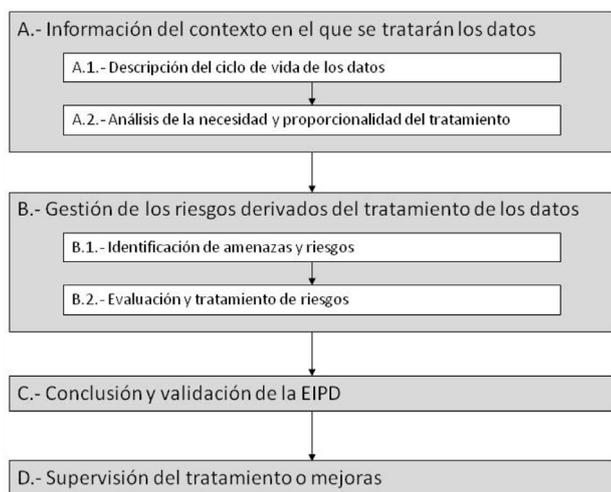


Figura 1. Apartados de la evaluación de impacto en protección de datos.

conseguir una población de pacientes simulados con técnicas de *machine learning*. La [figura 1](#) muestra los apartados de la EIPD, y en el [Apéndice online](#) se presenta la plantilla utilizada.

A. Información del contexto en el que se tratarán los datos

En este apartado se mostró cómo el tratamiento de los datos previsto era acorde a los principios del RGPD. Se describió el ciclo de vida de los datos y se analizó la necesidad y la proporcionalidad del tratamiento.

A.1. Descripción del ciclo de vida de los datos

Se detallaron las actividades a realizar, los datos específicos a tratar y las personas y las tecnologías implicadas; todo ello tanto para el proceso de adquisición de los datos como para su almacenamiento, tratamientos, cesiones a terceros y destrucción final.

Se especificaron las personas involucradas y sus roles, y se identificó al responsable del tratamiento (investigador principal), los encargados del tratamiento (miembros del equipo de investigación y personal técnico de tratamiento de datos), el delegado de protección de datos del centro donde se realiza la investigación y la persona responsable de los datos de la entidad que los suministra al equipo de investigación. En este proyecto no se contemplaba la figura de promotor del estudio. Sobre la entidad financiadora, la EIPD se realizó previamente a la presentación del proyecto a una convocatoria competitiva, y se presentó al Comité de Ética de la Investigación. Se especificó que no estaba previsto generar patentes, así como qué instrumentos se contaban para la protección de la propiedad y qué criterios se tendrían en cuenta en el uso secundario de los productos resultantes.

Respecto a la cesión de los datos por la entidad responsable (D.G. Asistencia Sanitaria y Resultados en Salud) al equipo de investigación, se indicó que está contemplado el uso de datos de salud para investigación sin necesidad de solicitar el consentimiento de la persona interesada, al tratarse en este caso de grandes bases de datos en las que la obtención de este consentimiento exige un esfuerzo desproporcionado respecto a los riesgos que pudiera suponer para la salvaguarda de la privacidad; además, el uso de estos datos es de interés público, de acuerdo con la Ley General de Sanidad, la Ley de Investigación Biomédica y la Ley General de Salud Pública.

La cesión se hace entre organismos dentro del Sistema Sanitario Público de Andalucía, en el contexto de un proyecto de investigación en el ámbito exclusivamente público. Se contempla la

transferencia de los datos mediante FTP entre servidores del anillo de salud de la Red Corporativa de la Junta de Andalucía.

En cuanto a los productos o servicios generados por el procesamiento de los datos, es preciso especificarlos, así como sus condiciones de uso y posible identificación o reidentificación de las personas.

En nuestro caso no se recogerían datos adicionales directamente de las personas incluidas en el estudio, por lo que no fue necesario especificar el procedimiento de información y solicitud de consentimiento. Los investigadores no disponían de la identificación personal de las personas, por lo que no se establecieron procedimientos para el ejercicio de los derechos por parte de los interesados (acceso, rectificación, cancelación/bloqueo, oposición y portabilidad). No estaba contemplado un tratamiento de datos fuera del Espacio Económico Europeo.

A.2. Análisis de la necesidad y proporcionalidad del tratamiento

Se hizo constar el informe sobre la legitimidad en el uso de bases de datos sin consentimiento informado en investigación sanitaria en determinadas circunstancias⁴, así como la legitimidad del uso de la Base Poblacional de Salud como infraestructura de investigación⁸.

En cuanto a la justificación, la necesidad del proyecto y del uso de los datos, se indicó que la generación de poblaciones de pacientes simulados trataría precisamente de evitar la reidentificación de pacientes anonimizados en proyectos de investigación⁹.

En este apartado se consignó el compromiso formal de usar los datos exclusivamente para la finalidad declarada. También se explicitó que los datos utilizados serían los mínimos imprescindibles para alcanzar los objetivos del proyecto, y el compromiso de mantener los datos sin destruir el tiempo estrictamente necesario.

B. Gestión de los riesgos derivados del tratamiento de los datos

En este apartado se identificaron, analizaron y valoraron la probabilidad y el impacto derivados de la posibilidad de que se materializaran en un riesgo, con el objetivo de establecer las acciones preventivas, correctivas y reductivas que permitieran minimizar la exposición al riesgo⁵.

B.1. Identificación de amenazas y riesgos

Para cada una de las actividades con los datos se identificaron las amenazas para la protección de datos y el riesgo al que pudieran someterse los derechos de las personas.

Los riesgos se presentaron en una matriz que tenía en cuenta la probabilidad y el impacto, valorados en cuatro niveles: despreciable, limitado, significativo o máximo. En nuestro proyecto, por ejemplo, una posible amenaza sería el acceso no autorizado, con riesgo de vulneración de derechos y libertades, que podría producir un daño moral o económico; sin embargo, con los mecanismos de seguridad con que contamos, tanto la probabilidad de que esto ocurra como su posible impacto son despreciables, por lo que el riesgo inherente es bajo.

B.2. Evaluar y tratar los riesgos

En este apartado es preciso identificar el riesgo inherente (riesgo intrínseco asociado a una actividad en sí misma) y el riesgo residual (riesgo de una actividad una vez aplicadas las medidas de control para mitigar o reducir la exposición al riesgo). En nuestro caso, como en otros muchos proyectos de investigación, no sería viable diferenciar ambos, al estar aplicadas por defecto las intervenciones de mitigación. Igualmente, en la mayoría de las EIPD no sería necesario realizar una consulta a la Autoridad de Control a través del Delegado de Protección de Datos, debido a que el riesgo residual sea alto o muy alto.

C. Conclusión y validación de la EIPD

Se incluyeron las conclusiones, y en este caso no era necesario un plan de acción. En las conclusiones se especificaron las posibles amenazas, su riesgo inherente y residual, y medidas de mitigación que podrían implantarse (para la mayoría de los proyectos, este aspecto no sería aplicable al estar solucionado por diseño).

D. Supervisión del tratamiento

La supervisión del tratamiento se asignó al investigador principal con el asesoramiento de expertos, y al delegado de protección de datos del centro. Es recomendable que este último participe en todo el proceso

Conclusiones

Aunque el RGPD y la LOPDGDD no afectan en principio a la disponibilidad de bases de datos para la investigación, sí introducen elementos nuevos, destinados a poder demostrar que el tratamiento de los datos es acorde a la normativa vigente.

La EIPD se configura como una pieza clave en la autorización del uso secundario de datos en investigación sanitaria, en la que el contexto del tratamiento toma gran relevancia respecto a las características de los datos. Consideramos que la EIPD debería ponerse a disposición de los comités de ética de la investigación en la evaluación de estos proyectos, previamente a su autorización.

La realización de una EIPD por parte de los investigadores es una oportunidad para reflexionar sobre la pertinencia de la investigación y para asegurar el cumplimiento de los principios de la protección de datos en un entorno cada vez más complejo y con mayores desafíos éticos.

Respecto a nuestra experiencia, no hemos encontrado dificultades en la descripción de todo el ciclo de vida de los datos. Ha resultado muy interesante la reflexión acerca de la necesidad y la proporcionalidad del tratamiento de los datos en el proyecto de investigación, y hemos encontrado más dificultades en el análisis de los riesgos derivados del tratamiento de los datos, para lo que ha sido de especial ayuda la guía de la AEPD.

Estas evaluaciones suponen una oportunidad de mejora de la calidad de los proyectos de investigación sanitaria a partir de bases de datos. Es deseable contar con personas integrantes o consultoras, expertas en aspectos éticos del tratamiento de datos, además de la colaboración imprescindible y cualificada del delegado de protección de datos, figura existente en todos los organismos públicos, centros sanitarios y universidades.

Editor responsable del artículo

Javier García Amez.

Contribuciones de autoría

Todas las personas firmantes han hecho contribuciones sustanciales a la concepción y el diseño del estudio, han participado en la redacción del artículo y han dado su aprobación al manuscrito enviado.

Financiación

Ninguna.

Conflicto de intereses

Ninguno.

Anexo. Material adicional

Se puede consultar material adicional a este artículo en su versión electrónica disponible en [doi:10.1016/j.gaceta.2019.10.006](https://doi.org/10.1016/j.gaceta.2019.10.006)

Bibliografía

1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (27 de abril de 2016).
2. Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales. (6 de Dic de 2018).
3. Sarrión-Esteve J, Benlloch-Domenech C. Una necesaria reflexión sobre el marco normativo de la investigación científica biomédica. *Gac Sanit.* 2019;33:93–4.
4. Informe 073667/2018. Madrid: Agencia Española de Protección de Datos. (Consultado el 4/7/2019.) Disponible en: <https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf>.
5. Gestiona EIPD. Madrid: Agencia Española de Protección de Datos. (Consultado el 2/10/2019.) Disponible en: <https://gestiona.aepd.es/>.
6. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetos al RGPD. Madrid: Agencia Española de Protección de Datos. (Consultado el 4/7/2019.) Disponible en: <https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf>.
7. Muñozerro-Muñoz D, Goicoechea-Salazar JA, García-León FJ, et al. Conexión de registros sanitarios: base poblacional de salud de Andalucía. *Gac Sanit.* 2019 May 25; pii: S0213-9111(19)30107-4.
8. Resolución 0068/18 de la Dirección Gerencia del Servicio Andaluz de Salud por la que se crea la Base Poblacional de Salud. Sevilla: Servicio Andaluz de Salud. (Consultado el 6/2/2010.) Disponible en: http://www.sas.junta-andalucia.es/principal/documentosacc.asp?pagina=pr_base_poblac.
9. De Lecuona I. Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (big data). *Gac Sanit.* 2018;32:576–8.