



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022



PROTECCIÓN DE DATOS Y ACCESO A LA HISTORIA CLÍNICA PARA INVESTIGACIÓN

Juan Díaz García

Delegado de Protección de Datos del SSPA

JORNADAS DE COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DE ANDALUCÍA

24 y 25 noviembre 2022

#ÉticaInvestigaciónAndalucía





INDICE:

Marco Legal - Introducción

Orden conjunta 1/2021

Garantías Técnicas y Organizativas

Evaluación del Cumplimiento en PD

Problemas con los Tratamientos de la Información

Accesos HCE

Conclusiones



**Estrategia
de Bioética**

del Sistema Sanitario
Público de Andalucía



DEFINICIONES

datos relativos a la salud: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;



DEFINICIONES

datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;



RGPD

Responsable del Tratamiento: Persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Director Gerente del SAS, Direcciones Generales y Directores de Centros.

Delegado de Protección de Datos: Informa y asesora al responsable o al encargado, supervisar el cumplimiento, asesora en las evaluaciones de impacto y actúa como punto de contacto de la autoridad de control.

Encargado del Tratamiento: Persona física o jurídica, autoridad pública, servicio u otro organismo que presta un servicio al responsable que conlleva el tratamiento de datos personales por cuenta de éste.



Protección de Datos desde el diseño

- **Medidas técnicas y organizativas adecuadas** (p.ej. seudonimización, minimización) para aplicar principios de PD de forma eficaz y proteger los derechos
- **En el momento de determinar los medios para el tratamiento y en el momento del tratamiento** (integrar necesarias garantías)
- Teniendo en cuenta
 - Naturaleza, ámbito, contexto y fines del tratamiento
 - Riesgos de diversa probabilidad y gravedad (no sólo alto riesgo)
 - Estado de la técnica y coste



Protección de Datos por defecto

- Medidas técnicas y organizativas apropiadas
- Tratamiento **por defecto sólo de datos personales necesarios para cada fin específico**
 - Cantidad de datos recopilados
 - Extensión del tratamiento
 - Periodo de almacenamiento
 - Accesibilidad
 - En particular, evitar la accesibilidad a un número indeterminado sin intervención de alguien



MARCO LEGAL I - Bases Jurídicas

RGPD Art 9 Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales ... de datos genéticos, datos biométricos,.. datos relativos a la salud.

Excepciones a la prohibición:

- a) el interesado dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
- i) el tratamiento es necesario por razones de interés público en el **ámbito de la salud pública**, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitario.
- j) el tratamiento es necesario con fines de archivo en interés público, **fines de investigación científica** o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros,

RGPD Art 6 Licitud del tratamiento

Consentimiento, Contrato, Obligación Legal, Intereses vitales, Interés público o Interés Legítimo.



MARCO LEGAL II – Investigación RGPD

Considerandos del RGPD – Interpretación:

159) El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de **manera amplia**, ...

157) **Combinando información procedente de registros**, los investigadores pueden obtener nuevos conocimientos de

gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. ... conocimientos sólidos y de alta calidad...

54) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales ... siempre que se den las garantías... fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad ... fines de **investigación científica** e histórica o fines estadísticos.

53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr dichos fines en **beneficio de las personas físicas y de la sociedad en su conjunto**,... fines de investigación ...

33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida... Los interesados deben tener la oportunidad de dar su **consentimiento solamente para determinadas áreas de investigación** o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.



Plazos Conservación

Ley Investigación Biomédica

Artículo 8. Trazabilidad y seguridad.

En el caso de la investigación con células y tejidos destinados a su aplicación en el ser humano, los datos para garantizar la trazabilidad deben conservarse durante al menos **treinta años**

Artículo 52. Conservación de los datos.

1. Los datos genéticos de carácter personal se conservarán durante un período mínimo de **cinco años** desde la fecha en que fueron obtenidos, transcurrido el cual el interesado podrá solicitar su cancelación.
2. Si no mediase solicitud del interesado, los datos se conservarán durante el plazo que sea necesario para preservar la salud de la persona de quien proceden o de terceros relacionados con ella.
3. Fuera de estos supuestos, los datos únicamente podrán conservarse, con fines de investigación, de forma anonimizada, sin que sea posible la identificación del sujeto fuente.



Plazos Conservación

Documento de instrucciones de la Agencia Española de Medicamentos y Productos Sanitarios para la realización de ensayos clínicos en España

Versión 17, de 18 de noviembre de 2022

¿Cuánto tiempo debe conservarse el **archivo maestro** de un ensayo autorizado con el Real Decreto 223/2004, de 6 de febrero, por el que se regulan los ensayos clínicos con medicamentos?

La legislación que aplica al período de custodia del archivo maestro desde la entrada en vigor del RD 1090/2015, de 4 de diciembre, es su art. 43, según el cual “1. El archivo maestro del ensayo clínico cumplirá con lo establecido en los artículos 57 y 58 del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014. Su contenido deberá tener en cuenta las orientaciones suplementarias al respecto publicadas por la Comisión Europea. 2. El promotor y el investigador conservarán el contenido del archivo maestro en formato papel o digital de cada ensayo clínico durante al menos **veinticinco años** tras la finalización del ensayo, o durante un período más largo si así lo disponen otros requisitos aplicables, como en el caso de que el estudio se presente como base para el registro de un medicamento en que se deberá cumplir el anexo I del Real Decreto 1345/2007, de 11 de octubre, o un acuerdo entre el promotor, el investigador y el centro.(...)”.



Disposición adicional decimoséptima. Tratamientos de datos de salud.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el **consentimiento** para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica.

Tales finalidades podrán abarcar **categorías relacionadas con áreas generales** vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en **vigilancia de la salud pública** podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos **para finalidades o áreas de investigación relacionadas** con el área en la que se integrase científicamente el estudio inicial

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.



Disposición adicional decimoséptima. Tratamientos de datos de salud.

d) Se considera lícito el uso de **datos personales seudonimizados** con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una **separación técnica y funcional** entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente **sean accesibles al equipo de investigación** cuando:

i) **Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.**

ii) Se **adopten medidas de seguridad específicas** para evitar la reidentificación y el acceso de terceros **no autorizados.**

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.



Disposición adicional decimoséptima. Tratamientos de datos de salud.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una **evaluación de impacto** que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las **normas de calidad** y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del **comité de ética de** la investigación previsto en la normativa sectorial.



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022



Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) [artículo 70, apartado 1, letra b)]

Adoptado el 23 de enero de 2019



RESOLUCIÓN CONJUNTA 1/2021 DE LA SECRETARÍA GENERAL DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN EN SALUD DE LA CONSEJERÍA DE SALUD Y FAMILIAS Y DE LA DIRECCIÓN GERENCIA DEL SERVICIO ANDALUZ DE SALUD POR LA QUE SE APRUEBAN INSTRUCCIONES PARA LA ORDENACIÓN DEL ACCESO Y USO DE LA INFORMACIÓN SANITARIA CONTENIDA EN LOS SISTEMAS DE INFORMACIÓN DEL SISTEMA SANITARIO PÚBLICO DE ANDALUCÍA CON FINES DE INVESTIGACIÓN E INNOVACIÓN POR LAS ENTIDADES DEPENDIENTES DE LA CONSEJERÍA DE SALUD Y FAMILIAS.

Instrucción primera: **Objeto de la instrucción**

1. El objeto de la presente Instrucción es establecer el **procedimiento** para que las personas o entidades investigadoras puedan solicitar el acceso y/o **uso de información sanitaria** que se encuentra bajo la custodia del Servicio Andaluz de Salud para la investigación e innovación en salud, y las condiciones para su autorización.



Personas o entidades solicitantes

1. Podrán solicitar acceso y/o uso de la información contenida en los sistemas indicados en el punto Primero de la Instrucción las personas investigadoras principales o investigadoras responsables (IP o IR) de un proyecto de investigación clínica y/o sanitaria debidamente informado por un Comité de Ética de la Investigación, que formen parte de las siguientes entidades públicas:

a) Los centros asistenciales del SSPA y de los distintos departamentos de la CSAFA y del SAS

b) Las entidades instrumentales en materia de investigación dependientes de la CSAFA

2. Las solicitudes de investigadores de otras entidades están fuera del alcance de estas instrucciones sin perjuicio de que se pueda establecer un convenio entre las entidades promotoras del estudio de investigación y el SAS/CSAFA.



Documentación requerida

1. Las solicitudes se presentarán cumplimentando el modelo “Solicitud de Acceso/Usos de información sanitaria del SSPA con fines de investigación e innovación” incluido en el Anexo 2 y disponible tanto en la web de la CSAFA como en la del SAS.
2. A este modelo de solicitud deberá acompañarse la siguiente documentación preceptiva:
 - A. Proyecto de Investigación e Innovación
 - B. Consentimiento informado
 - C. Ente financiador o promotor
 - D. Dictamen de aprobación del CEI
 - E. Evaluación de Impacto en Protección de Datos
 - F. Declaración responsable de confidencialidad y no reidentificación
 - G. Declaración responsable de no cesión de los datos a terceros
 - H. Declaración responsable de la no transferencia fuera del ámbito de aplicación del RGPD
 - I. Documento de relación contractual de encargo de tratamiento de los datos.



Garantías Técnicas y Organizativas

RGDP - Principio de Responsabilidad proactiva

Tipos de medidas

- Mantener “registro de actividades de tratamiento”
- Medidas de Protección de Datos desde el Diseño
- Medidas de Protección de Datos por Defecto
- Aplicar medidas de seguridad adecuadas
- Llevar a cabo Evaluaciones de Impacto
- Autorización previa o consultas previas con APD
- Designación Delegado Protección de Datos (DPD)
- Notificación de Quiebras de Seguridad
- Códigos de conducta y esquemas de certificación





Mapa de roles en Ensayos Clínicos

RESPONSABLES del TRATAMIENTO

TRATAMIENTOS DE INVESTIGACIÓN

CUADERNO DE RECOGIDA DE DATOS

DG Asistencia Sanitaria
Centro Sanitario
Investigador Principal

Promotor

Datos Identificados



Datos Pseudonimizados



ENCARGADOS del TRATAMIENTO

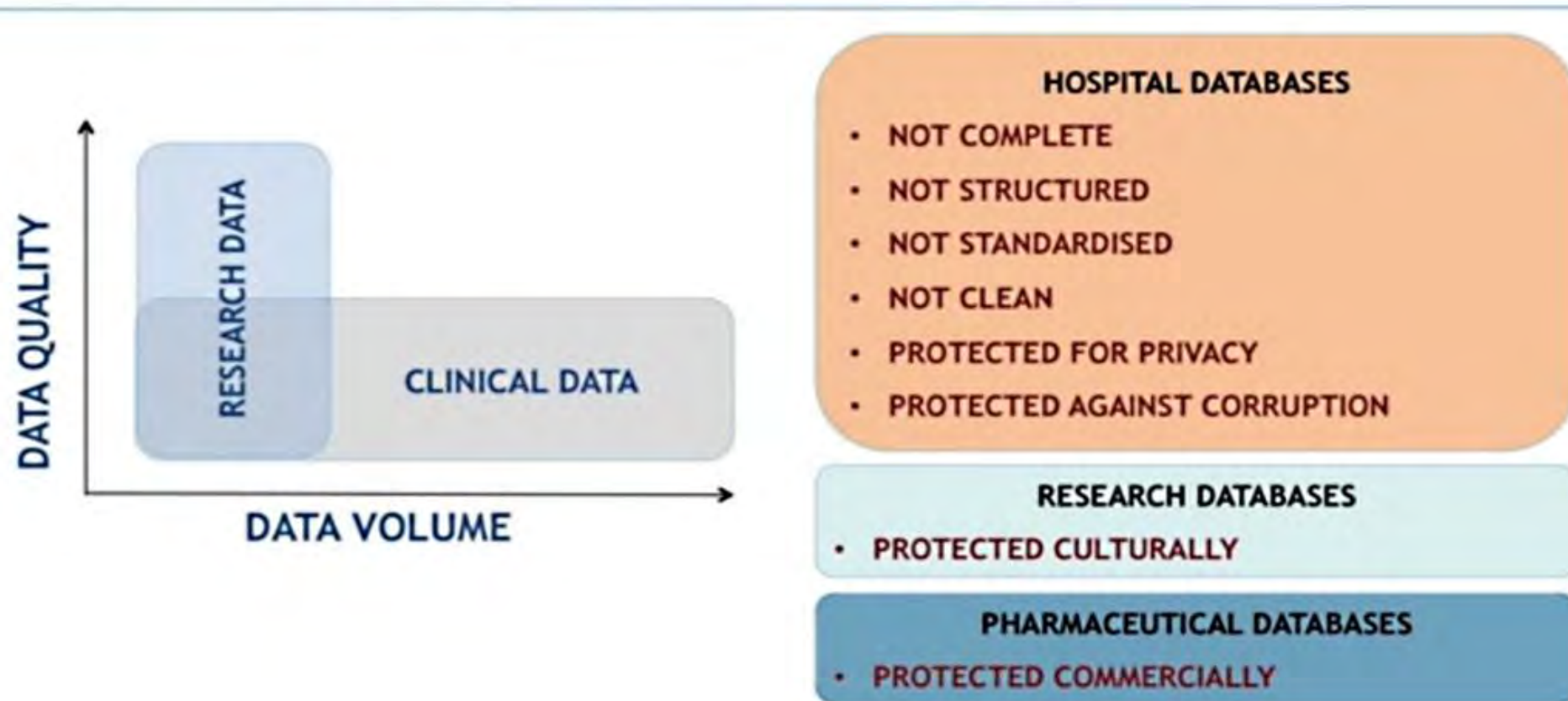
Fundaciones Gestoras I+D+i
Investigadores contratados

CRO
Monitor
Auditor



Problemas en los Tratamientos de la Información

DATA SOURCES AND CHALLENGES





EVOLUCIÓN MEDIDAS DE SEGURIDAD Y ORGANIZATIVAS





Medidas básicas

ESQUEMA NACIONAL DE SEGURIDAD 75 MEDIDAS DE SEGURIDAD

MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad



- POLÍTICA DE SEGURIDAD
- NORMATIVA DE SEGURIDAD
- PROCEDIMIENTOS DE SEGURIDAD
- PROCESO DE AUTORIZACIÓN

MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin



- PLANIFICACIÓN
- CONTROL DE ACCESO
- EXPLOTACIÓN
- SERVICIOS EXTERNOS
- CONTINUIDAD DEL SERVICIO
- MONITORIZACIÓN DEL SISTEMA

MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.



- INSTALACIONES E INFRAESTRUCTURAS
- GESTIÓN DEL PERSONAL
- PROTECCIÓN DE LOS EQUIPOS
- PROTECCIÓN DE LAS COMUNICACIONES
- PROTECCIÓN SOPORTES DE INFORMACIÓN
- PROTECCIÓN APLICACIONES INFORMÁTICAS
- PROTECCIÓN DE LA INFORMACIÓN
- PROTECCIÓN DE LOS SERVICIOS

Protección de Datos desde el diseño

Protección de Datos por defecto



PRIVACY BY DESIGN

A VISUAL GUIDE TO PRACTICAL DATA DE-IDENTIFICATION

Usabilidad de la Información



What do scientists, regulators and lawyers mean when they talk about de-identification? How does anonymous data differ from pseudonymous or de-identified information? Data identifiability is not binary. Data lies on a spectrum with multiple shades of identifiability.



This is a primer on how to distinguish different categories of data.

DEGREES OF IDENTIFIABILITY

Information containing direct and indirect identifiers.

PSEUDONYMOUS DATA

Information from which direct identifiers have been eliminated or transformed, but indirect identifiers remain intact.

DE-IDENTIFIED DATA

Direct and known indirect identifiers have been removed or manipulated to break the linkage to real world identities.

ANONYMOUS DATA

Direct and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.

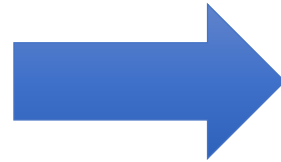
	EXPLICITLY PERSONAL	POTENTIALLY IDENTIFIABLE	NOT READILY IDENTIFIABLE	KEY CODED	PSEUDONYMOUS	PROTECTED PSEUDONYMOUS	DE-IDENTIFIED	PROTECTED DE-IDENTIFIED	ANONYMOUS	AGGREGATED ANONYMOUS
DIRECT IDENTIFIERS Data that identifies a person without additional information or by linking to information in the public domain (e.g., name, SSN)	INTACT	PARTIALLY MASKED	PARTIALLY MASKED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
INDIRECT IDENTIFIERS Data that identifies an individual indirectly. Helps connect pieces of information until an individual can be singled out (e.g., DOB, gender)	INTACT	INTACT	INTACT	INTACT	INTACT	INTACT	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED	ELIMINATED or TRANSFORMED
SAFEGUARDS and CONTROLS Technical, organizational and legal controls preventing employees, researchers or other third parties from re-identifying individuals	NOT RELEVANT due to nature of data	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	LIMITED or NONE IN PLACE	CONTROLS IN PLACE	NOT RELEVANT due to nature of data	NOT RELEVANT due to high degree of data aggregation
SELECTED EXAMPLES	Name, address, phone number, SSN, government-issued ID (e.g., Jane Smith, 123 Main Street, 555-555-5555)	Unique device ID, license plate, medical record number, cookie, IP address (e.g., MAC address 68:A8:6D:35:65:03)	Same as Potentially identifiable except data are also protected by safeguards and controls (e.g., hashed MAC addresses & legal representations)	Clinical or research datasets where only cursor retains key (e.g., Jane Smith, diabetes, Hg8 15.1 g/dl = Crk123)	Unique, artificial pseudonyms replace direct identifiers (e.g., HIPAA Limited Datasets, John Doe = 5L7T LX619Z) (unique sequence not used anywhere else)	Same as Pseudonymous, except data are also protected by safeguards and controls	Data are suppressed, generalized, perturbed, swapped, etc. (e.g., GPA: 3:2 = 3.0-3.5, gender: female = gender: male)	Same as De-identified, except data are also protected by safeguards and controls	For example, noise is calibrated to a data set to hide whether an individual is present or not (differential privacy)	Very highly aggregated data (e.g., statistical data, census data, or population data that 52.6% of Washington, DC residents are women)



PSEUDONIMIZACIÓN

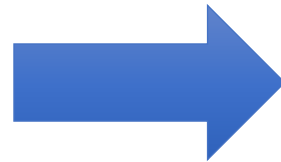
¿QUIÉN PSEUDONIMIZA?

- Basada en Consentimiento Retrospectivos Ensayos Clínicos



Investigador
Mantiene la Reversibilidad

- Basada en DA 17ª



Equipo Separado
Técnico y Funcional
Mantiene la Reversibilidad





ANONIMIZACIÓN

Orientaciones y
garantías
en los
procedimientos de
ANONIMIZACIÓN
de datos
personales





RIESGOS DE LA ANONIMIZACIÓN

ARTICLE 29 DATA PROTECTION WORKING PARTY



0829/14/EN
WP216

Opinion 05/2014 on Anonymisation Techniques

Adopted on 10 April 2014

El grupo de trabajo del Artículo 29 (GT29) define que es necesario realizar una evaluación de las técnicas y procedimientos de anonimización utilizados, a fin de acreditar que la disociación realizada evita que:

- (i) se pueda **identificar** a una persona física dentro de un conjunto de datos;
- (ii) se pueda **relacionar o enlazar** la información de una persona física a partir de la vinculación de dos registros dentro de un conjunto de datos (o entre dos conjuntos de datos independientes); o
- (iii) se pueda **inferir** cualquier información sobre la persona.



REIDENTIFICACIÓN

Re-identification possible with Australian de-identified Medicare and PBS open data

Using publicly known information, a team of researchers from the University of Melbourne have claimed to re-identify seven prominent Australians in an open medical dataset.

By [Chris Duckett](#) | December 18, 2017 -- 01:01 GMT (01:01 GMT) | Topic: [Security](#)

HEALTH DATA IN AN OPEN WORLD

A REPORT ON RE-IDENTIFYING PATIENTS IN THE MBS/PBS DATASET AND THE IMPLICATIONS FOR FUTURE RELEASES OF AUSTRALIAN GOVERNMENT DATA

Chris Culnane, Benjamin Rubinstein and Vanessa Teague

School of Computing and Information Systems

The University of Melbourne, 18 Dec 2017

{christopher.culnane, benjamin.rubinstein, vjteague}@unimelb.edu.au



REIDENTIFICACIÓN

La reidentificación es un proceso continuo que necesita reevaluar los escenarios de ataque cada vez que se dispone de datos adicionales de diferentes fuentes.



Los investigadores de la Universidad Carnegie Mellon descubrieron que era posible identificar al 87 por ciento de la población estadounidense del censo de 1990 sólo con el código postal, el sexo y la fecha de nacimiento



REIDENTIFICACIÓN

Los métodos más frecuentes en los ataques son:

Identificación: aislar algunos o todos los registros pertenecientes a un titular de datos en el conjunto de datos mediante la observación de un conjunto de características que se sabe que identifican de forma exclusiva a este titular de datos.

Vinculación: asociar registros relativos al mismo principal de datos o a un grupo de principales de datos en conjuntos de datos separados.

Inferencia: deducir con una probabilidad no despreciable el valor de un atributo a partir de los valores de un conjunto de otros atributos.



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022



Datos Identificados

Máxima Utilidad
Maximo Riesgo



Datos Pseudonimizados

Utilidad Aceptable
Riesgo Aceptable



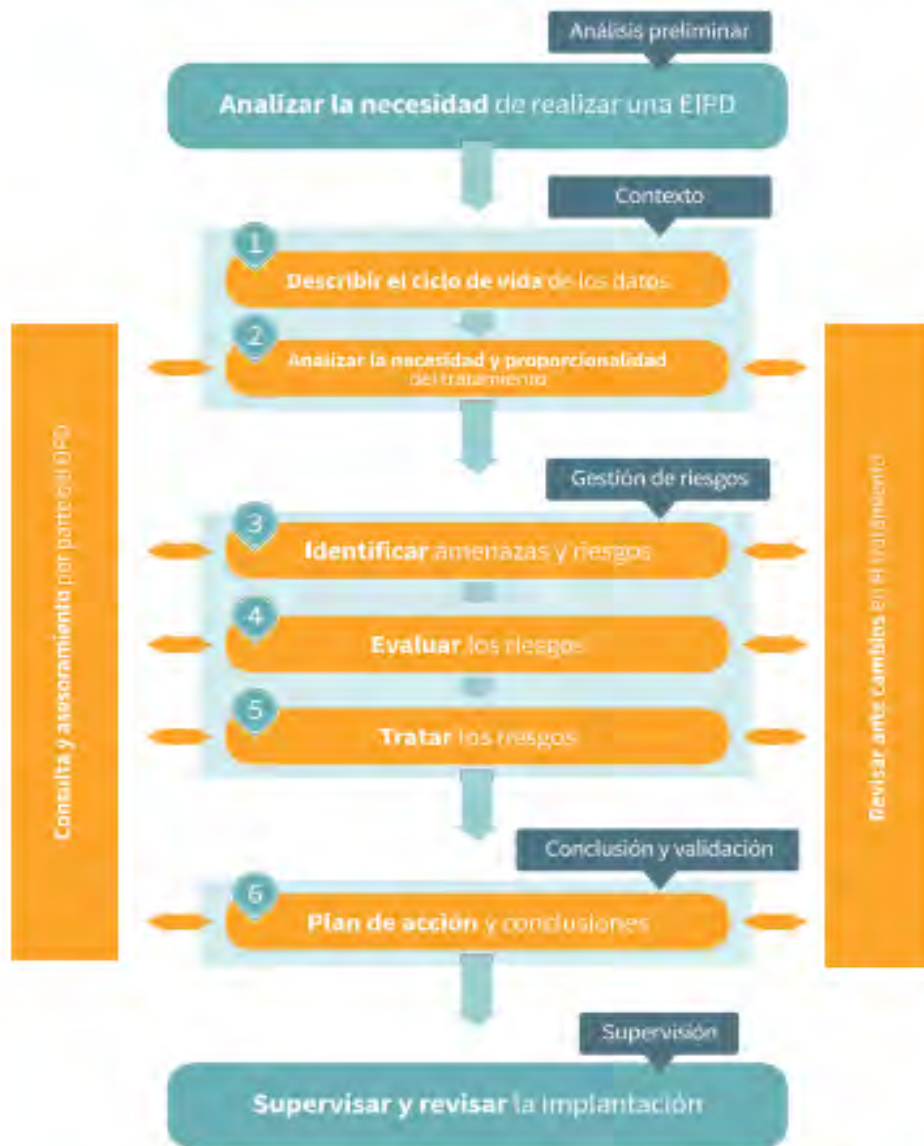
Datos Anonimizados

Mínima Utilidad
Mínimo Riesgo



Evaluación de impacto

- Deberá realizarse cuando sea probable que el tratamiento previstos presente **un alto riesgo específicos para los derechos y libertades** de los interesados, entre otros casos, cuando:
 - elaboración de **perfiles** sobre cuya base se tomen **decisiones** que produzcan **efectos jurídicos** para las personas físicas o que les afecten significativamente de modo similar;
 - tratamiento a **gran escala** de las **categorías especiales de datos**
 - **observación sistemática a gran escala** de una zona de acceso público
- Las APD **deberán** establecer listas adicionales de tratamientos de alto riesgo y **podrán** establecer listas que no requieren EIPD
- El RGPD prevé un **contenido mínimo** de la evaluación
- **Como novedad, se prevé que habrá de recabarse “cuando proceda” la opinión de los interesados**







EVALUACIONES DE IMPACTO DE P.D.

FASE	Responsable del tratamiento	DPD	Encargado del tratamiento	Otras áreas relevantes (pe seguridad, riesgos, Asesoría Jurídica, ...)
1 Describir el ciclo de vida de los datos	R/A	C/I	C	C
2 Analizar la necesidad y proporcionalidad del tratamiento	R/A	C/I	C	C
3 Identificar amenazas y riesgos	R/A	C/I	C	-
4 Evaluar los riesgos	R/A	C/I	C	-
5 Tratar los riesgos	R/A	C/I	C	C
6 Plan de acción y conclusiones	R/A	C/I	C	C



JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022

 Tipo de amenaza	Identificación	¿Qué preguntas se pueden formular para identificar la amenaza?
 Acceso ilegítimo a los datos	<ul style="list-style-type: none"> ● Pérdidas de dispositivos móviles ● Fuga de información ● Acceso intencionado por parte de personal no autorizado ● Ataques intencionados (hacking, suplantación de identidad, etc.) ● Uso ilegítimo de datos personales 	<ul style="list-style-type: none"> ¿Los dispositivos móviles y de almacenamiento están cifrados? ¿Existen métodos para extraer la información durante la operación de tratamiento? ¿Está expuesta la información al acceso por parte de terceros no autorizados? ¿Existe un mecanismo para dar acceso a los datos únicamente al personal autorizado? ¿La operación de tratamiento es susceptible de ataques de hacking? ¿es susceptible de ataques de phishing o de otros métodos de suplantación de identidad? ¿Existe una adecuada gestión de la configuración de los parámetros de seguridad de los elementos (elementos de red, SO y BBDD)? ¿Existe una base legitimadora para la actividad de tratamiento? ¿las finalidades de las actividades de tratamiento son necesarias y proporcionales?
 Modificación no autorizada de los datos	<ul style="list-style-type: none"> ● Ataque para la suplantación de identidad ● Errores en los procesos de recopilación y captura de información ● Modificación no autorizada de datos intencionada ● Uso ilegítimo de datos personales 	<ul style="list-style-type: none"> ¿Existen credenciales o mecanismos de control que limiten el acceso a personal no autorizado? ¿Se revisa periódicamente la actividad realizada por los usuarios cuando acceden a los sistemas? ¿Existen controles sobre la integridad de la información durante el proceso de captura de datos? ¿se identifica adecuadamente al interesado que proporciona los datos? ¿Los datos son modificables únicamente por el personal autorizado? ¿La actividad de tratamiento sobre los datos son acordes a las finalidades para las cuales existe una base legitimadora? ¿se puede realizar un perfilado o una operación de tratamiento que no esté alineada con las finalidades de la operación de tratamiento?
 Eliminación de los datos	<ul style="list-style-type: none"> ● Corte de suministro eléctrico o fallos en servicios de comunicaciones ● Error humano o ataque intencionado que provoca borrado o pérdida de datos ● Desastres naturales 	<ul style="list-style-type: none"> ¿Un fallo de suministro eléctrico puede implicar la pérdida de datos? ¿Un fallo en los servicios de comunicaciones puede ocasionar una pérdida de datos? ¿Los datos pueden ser eliminados únicamente por el personal autorizado? ¿Existen copias de seguridad? ¿Están los sistemas que almacenan datos en ubicaciones expuestas a la posibilidad de que se produzca un desastre natural? ¿Existe réplica de los datos en diferentes ubicaciones?



Evaluación Impacto de Protección de Datos

Obligación del Responsable del Tratamiento - para garantizar que el tratamiento se realiza de acuerdo RGPD

Se realiza antes de tratar los datos , permite detectar riesgos y corregirlos

Es obligatoria desde 2018

Metodología AEPD

Herramientas de uso general



Problemas: ¿Quién?, ¿Cuándo?

EPID – grupo de revisión – equipo multidisciplinar – investigador – tic – legal - clínico

Difícil de comprender por el personal investigador

Para el responsable de sistema

Falta de perspectiva de investigación en la metodología

Valoración subjetiva de las medidas y riesgos

No enfocado a proyectos Big Datos, Inteligencia Artificial o Plataformas distribuidas

Visión inicial del proyecto – no recoge cambios en la vida del proyecto



Evaluación del Cumplimiento PD

DPD Salud Cataluña. Guía de evaluación de la normativa de Protección de Datos en proyectos de Investigación

Guía informativa de los principales aspectos que en materia de protección de datos se tendrán en cuenta a la hora de evaluar proyectos de investigación, tanto por el miembro experto en protección de datos de los CEI o CEIM, como por los evaluadores.

Guia d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca

Sota d'avaluació dels aspectes derivats de la normativa de Protecció de Dades en projectes de recerca
Departament de Salut

31 de juliol de 2020

Departament de Salut i Departament de Salut de Catalunya

Sumari

- 1. Objectius del document..... 4
- 2. Intenció..... 4
- 3. Contexte legal de protecció de dades i la seva aplicació en l'àmbit de recerca..... 4
- 3.1. Definició de les dades i de dades personals..... 5
- 3.2. Règim de tractament de les dades..... 7
- 3.3. Finalitat de les dades i per finalitat..... 7
- 3.4. Finalitat de tractament de les dades..... 8
- 3.5. Finalitat d'informació..... 8
- 3.6. Drets legítims i tipus de tractament de dades per informació..... 9
- 3.7. Responsabilitat legal, delegació de tractament i subtercessió internacional..... 10
- 3.8. Dependència en el tractament de dades amb finalitat de recerca..... 10
- 3.9. Retenció i destrucció internacional..... 11
- 3.10. Aspectes que s'han d'incloure en el protocol de recerca de dades de la perspectiva de la protecció de dades..... 11
- 3.11. Metodologia per avaluar els aspectes derivats de la normativa de protecció de dades en projectes de recerca..... 11
- 4. Annexos i referències..... 12

4 Aspectes que s'han d'incloure en el protocol dels projectes de recerca des de la perspectiva de la protecció de dades

El CEI, quan revisa projectes de recerca, han de garantir que el tractament de les dades en el marc del projecte complix els requisits del RGPD i de la LOPD-BUO.

Amb aquesta Guia, quan es presenta un projecte de recerca, s'ha d'adjuntar un apartat específic on es detallen tots els aspectes relacionats amb el tractament de dades personals. A tal efecte, s'haurà de garantir que el document d'informació i consentiment que signen els participants en un projecte de recerca, conté tota la informació relativa al tractament de dades en el marc del projecte de recerca i la consentiment per al participant, així com tota la informació relativa a l'obtenció del seu dret de consentiment i tractament de dades que es dugui a terme en el marc de l'activitat de recerca.

El CEIM quan revisi els protocols dels projectes de recerca han de revisar que contengui tots els elements que es detallen a continuació:

Taula 1. Informació que ha d'incloure un protocol d'un projecte de recerca.

Item a revisar	Informació que s'ha d'aportar al protocol
Identificació del responsable del tractament	<ul style="list-style-type: none"> • Cal identificar quins entitat és la responsable del tractament, les dades de contacte, la forma de contacte amb el seu Delegat de Protecció de Dades i la forma d'exercici dels drets. • En cas de constar una situació de coresponsabilitat, cal que s'inclogui en les dades del document de consentiment, així com la designació de la part de tractament responsable en cada coresponsabilitat. • Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.

Principals del tipus de dades que es tractaran i la forma com es tractaran	<ul style="list-style-type: none"> • Una d'aportar informació en relació amb els tipus de dades que es tractaran (identificatives, sanitàries, genòmiques, biomètriques, ...). • Una d'aportar informació en relació amb la forma com es tractaran aquestes dades (identificades, codificades, pseudonimitzades o anonimitzades). Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca. • Indicar si les dades estan codificades, pseudonimitzades o anonimitzades, s'ha d'especificar la forma com es fan així. • Una d'aportar informació en relació amb el temps de conservació de les dades. Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.
Origen de les dades i legitimitat per al seu tractament	<ul style="list-style-type: none"> • Una d'aportar informació en relació amb el origen de les dades en el marc del projecte de recerca, així com la base de legitimitat per a la seva utilització. Les dades poden provenir: <ul style="list-style-type: none"> ✓ Directament del titular en el marc del projecte de recerca mèdica. ✓ De tractaments anteriors (reutilització de dades). ✓ Aquesta informació s'haurà de reflectir al full d'informació del participant al projecte de recerca.
Mínimisme	<ul style="list-style-type: none"> • Si es recullen els dades mínims necessaris per assolir els objectius de recerca, és a dir que no es recullen més dades de les necessàries. • Si s'ha considerat la possibilitat d'utilitzar dades anònimes o pseudonimitzades. • El protocol del projecte ha de detallar totes les comunicacions de dades que es produeixin en el marc del projecte i la seva legitimitat. Caldrà distingir i detallar la presència de: <ul style="list-style-type: none"> ✓ Comunicacions de tractament (art. 28 RGPD). ✓ Comunicacions de tractament de dades (art. 44 e 45 RGPD). ✓ Altres comunicacions de dades.
Comunicacions de dades	<ul style="list-style-type: none"> • La informació relativa a l'existència o de comunicacions i la transferència internacional de dades s'haurà de reflectir al full d'informació del participant al projecte de recerca.

Sistema de tractament de la informació	<ul style="list-style-type: none"> • El protocol ha d'indicar les eines informàtiques que s'utilitzaran per al tractament de les dades, ja siguin tant de tipus institucional com no institucional, indicant tant de forma específica i detallada els següents aspectes: <ul style="list-style-type: none"> ✓ Us de sistemes o emmagatzemament en núvol. ✓ Us de dispositius. ✓ Us d'aparells connectats o dispositius portàtils. ✓ Si es realitzaran, transmissió i emmagatzemament de dades de categoria personal i categories especials de forma segura. ✓ Si el nivell de seguretat proporcionat és adequat per als riscos que comporta el tractament. ✓ Si es preveuen en marxa procediments per a l'eliminació de la informació segura de dades personals o dades de categoria especial quan ja no es necessitin.
Avaluació d'impacte	<ul style="list-style-type: none"> • Una d'aportar informació en relació amb els resultats de l'avaluació d'impacte que s'ha realitzat i el tractament de dades del projecte de recerca. • Si l'avaluació d'impacte determina que el tractament impliqui un alt risc per als titulars de les dades, s'hauran d'indicar les mesures que s'han pres per mitigar-lo.
Legitimitat de les mesures preses en relació amb els tractaments que poden afectar un alt risc per als drets i les llibertats dels participants en la investigació	<ul style="list-style-type: none"> • El protocol ha d'indicar si es donen les situacions que es detallen a continuació, i la forma com s'han mitigat els riscos: <ul style="list-style-type: none"> ✓ Realització de posttestos de dades o prova de decisions automatitzades respecte participants individuals. ✓ Ús d' eines de intel·ligència artificial. ✓ Utilització de tecnologies d'anonimització de dades amb tecnologies Big Data. ✓ Utilització de sistemes de autoseguretat. ✓ Utilització de sistemes de pseudonimització.

Aquesta informació s'ha de proporcionar als investigadors i als titulars de dades que estiguin involucrats al protocol i al full d'informació i consentiment (en cas que n'hi hagi).

Aquesta Guia es pot adaptar per a cada centre a l'efecte que es detallen els seus requisits a tots els investigadors i promotores.



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Identificación del responsable del tratamiento	<p>Hay que identificar qué entidad es la responsable del tratamiento , los datos de contacto, la forma de contacto con su Delegado de Protección de Datos y la forma de ejercicio de los derechos.</p> <p>En caso de darse una situación de corresponsabilidad, es necesario que se indiquen los datos de los dos corresponsables, así como la descripción de la parte de tratamiento realizada por cada corresponsable.</p> <p>Esta información se deberá reflejar en la hoja de información del participante al proyecto de investigación.</p>



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Descripción del tipo de datos que se tratarán y de la forma como se tratarán	<p>Se debe aportar información en relación con las tipologías de datos que se tratan (identificativos, hábitos, salud, genéticas, biométricas ...), y si es posible las variables concretas.</p> <p>Se debe aportar información en relación con la forma como se tratarán estos datos (identificadas, codificadas, pseudonimizadas o anonimizadas).</p> <p>Esta información se deberá reflejar en la hoja de información del participante al proyecto de investigación.</p> <p>Se debe aportar información en relación con el tiempo de conservación de los datos.</p> <p>Esta información se deberá reflejar en la hoja de información del participante al proyecto de investigación.</p>



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Origen de los datos y legitimación para su tratamiento	<p>Se indicará <u>de donde provienen</u> los datos que se utilizarán en el marco del proyecto de investigación, así como la <u>base de legitimación</u> para su utilización.</p> <p>Los datos pueden provenir:</p> <ul style="list-style-type: none">* Directamente del titular en el marco del proyecto de investigación concreto.* De tratamientos preexistentes (reutilización de datos). <p>La base de legitimación ha de expresarse conforme al art. 6 del RGPD.</p> <p>Esta información se deberá reflejar en la hoja de información del participante al proyecto de investigación.</p>



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Minimización	<p>Si se recogen los ítems mínimos necesario para alcanzar los objetivos de investigación, es decir que no se recogen más datos de los necesarios.</p> <p>Si se ha considerado la posibilidad de utilizar datos anónimos o seudonimizados. En su caso justificación de los motivos por los que se ha descartado.</p>



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Comunicación de datos	<p>El protocolo del proyecto debe detallar todas las comunicaciones de datos que se producen en el marco del proyecto, y su legitimación. Habrá que distinguir e indicar la existencia de:</p> <ul style="list-style-type: none">* Encargados de tratamiento (art. 28 RGPD)* Transferencias internacionales de datos (art. 44 a 45 RGPD)* Otras comunicaciones de datos (p.e: promotor, registros nacionales/internacionales,...) <p>La información relativa a la existencia de comunicaciones y la transferencia internacional de datos deberá reflejarse en la hoja de información del participante al proyecto de investigación.</p>



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Sistemas de tratamiento de la información	<p>El protocolo debe indicar las herramientas informáticas que se utilizan para el tratamiento de los datos, ya sean institucionales/corporativas o no (externas), indicándolo de forma específica y describiendo los siguientes supuestos:</p> <ul style="list-style-type: none">* Uso de sistemas de almacenamiento en la nube* Uso de wearables* Uso de apps sometidas a cláusulas generales* Si se recopilarán, transmitirán y almacenarán datos de categoría personal / categorías especiales de forma segura.* Si el nivel de seguridad proporcionado es adecuado para los riesgos que representa el tratamiento.* Si se pondrán en marcha procedimientos para la eliminación y / o la destrucción segura de datos personales o datos de categoría especial cuando ya no se necesiten.



Evaluación del Cumplimiento de PD

Ámbito	Elementos de detalle
Evaluación de impacto	<p>Se debe aportar información en relación con los resultados de la evaluación de impacto que se ha realizado del tratamiento de datos del proyecto de investigación.</p> <p>Si la evaluación de impacto determina que el tratamiento implica un alto riesgo para los titulares de las datos, se deberán indicar las medidas tomadas para mitigarlo.</p>



Cumplir los principios de protección de datos personales NO [solo] es:

- Pedir el consentimiento para el tratamiento de los datos (p.e: acceso a la HC).
Incluida revocación.
- Pedir al CEI/CEIm la exención del consentimiento informado.
- Indicar en la memoria que se emplearán datos anónimos.
- Mencionar la normativa de protección de datos personales en la memoria del proyecto.
- Incluir a un tutor sanitario como canal de acceso a los datos en un TFG/TFM.
- Incluir como parte del equipo de investigación al personal del servicio de informática del centro sanitario
encargado de la extracción de los datos.
- Escudarse en una situación de emergencia sanitaria.
- Etc.



Problemas en los Tratamientos de la Información

Problemas de Procedimientos - ciclo de vida – DMP data management plant

Problemas Metodológicos – estadísticos

Problemas con las Herramientas – Nube (cambio herramientas por datos) cesiones de datos

Procesamiento de lenguaje natural – Fuente de Información

Proyectos de datos masivos para entrenar Algoritmos

Problemas Big data / IA- caja negra – Explicabilidad – Sesgos - Estándares

Investigadores / Reclutadores / Promotores / Sociedades Científicas

Riesgos:

Trasferencias internacionales

Pruebas de algoritmos – formato de suscripción -

Ubicación de los algoritmos

Cesiones de datos ocultas

Indefinición de Contratos de Encargo de Tratamiento

Necesidad de las Clausulas Contractuales Tipo

IA federados - Calculo local - Modelos distribuidos





JORNADA DE LOS COMITÉS DE ÉTICA DE LA INVESTIGACIÓN DEL SSPA - 2022





EU initiative on a European Health Data Space (EHDS)

eHealth Stakeholder Group – towards EHDS acceptance

The eHSG have formed 5 working groups on which concrete solutions the stakeholders identify and actions that could be taken in the area of:



- 1. promoting access to health data and interoperability*
- 2. re-use of health data for research and policy-making*
- 3. promotion of digital health services and products*
- 4. uptake of AI for health*
- 5. sharing of data between public and private partners*

El espacio europeo será clave para tres ejes esenciales de la protección de la salud pública: la prestación de asistencia sanitaria; la investigación y la elaboración de políticas sanitarias; y el sistema de alerta temprana sobre amenazas transfronterizas de salud”.



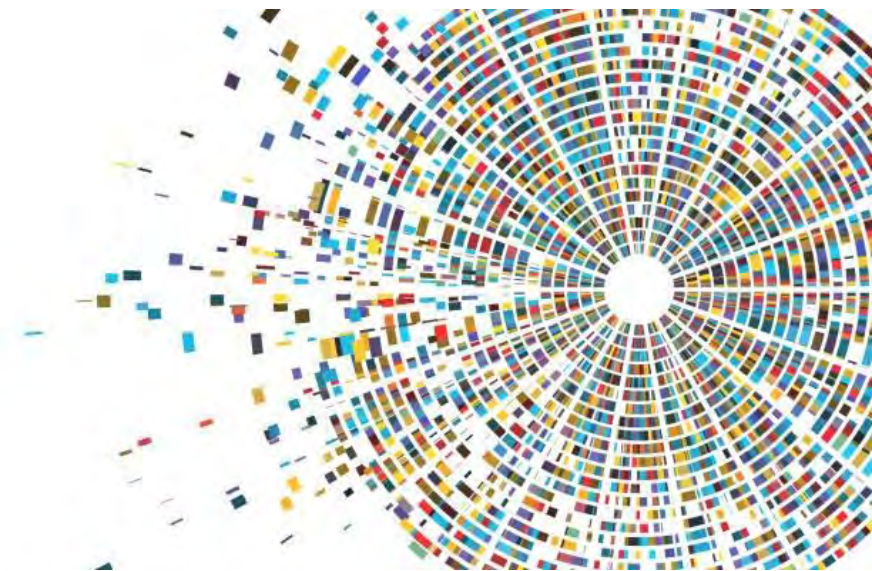
'Red.es' adjudica por 4,6 millones de euros una solución de analítica avanzada para la sanidad pública andaluza



El programa tenía un precio de licitación de 7,7 millones de euros, por lo que la adjudicación supone un ahorro de casi el 40%. - Red.es

SEVILLA, 3 Ago. (EUROPA PRESS) -

'Red.es', entidad pública empresarial adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, ha adjudicado este martes el 'Servicio para la implantación de una solución corporativa de analítica avanzada', basada en tecnologías 'big data', para el Sistema Sanitario Público de Andalucía a la UTE EY Transforma Servicios de Consultoría por un importe de 4,6 millones de euros.





Formación básica en protección de datos

Protección de datos personales desde el puesto de trabajo.

Ámbito: SAS

Inscripción: Gesforma SSCC

- 5 horas, online tipo MOOC, 1 ed./mes

Contenidos:

- U.D.0: Introducción
- U.D.1: Pilares de la protección de datos personales.
- U.D.2: Relación de actividades profesionales afectadas por la protección de datos
- U.D.2: Técnicas y herramientas garantes del cumplimiento
- U.D.4: Brechas de seguridad





CONCLUSIONES

- Procesos Multidisciplinar – Informática – Estadística - Investigación - Clínica
- Riesgos de la Reidentificación
- Separación Técnica y Funcional
- Formación – Confusión de conceptos – Legislación Compleja
- Medidas de Seguridad técnicas y organizativas para la Investigación
- Necesidades de Plataformas especializadas en Investigación
- Procedimientos Pseudo/Anonimización en extracción de datos para investigación.
- Metodología en Evaluaciones de Impacto en BD e IA
- Papel de apoyo de los CEIs o DGAS-Gestión Sistemas de Información



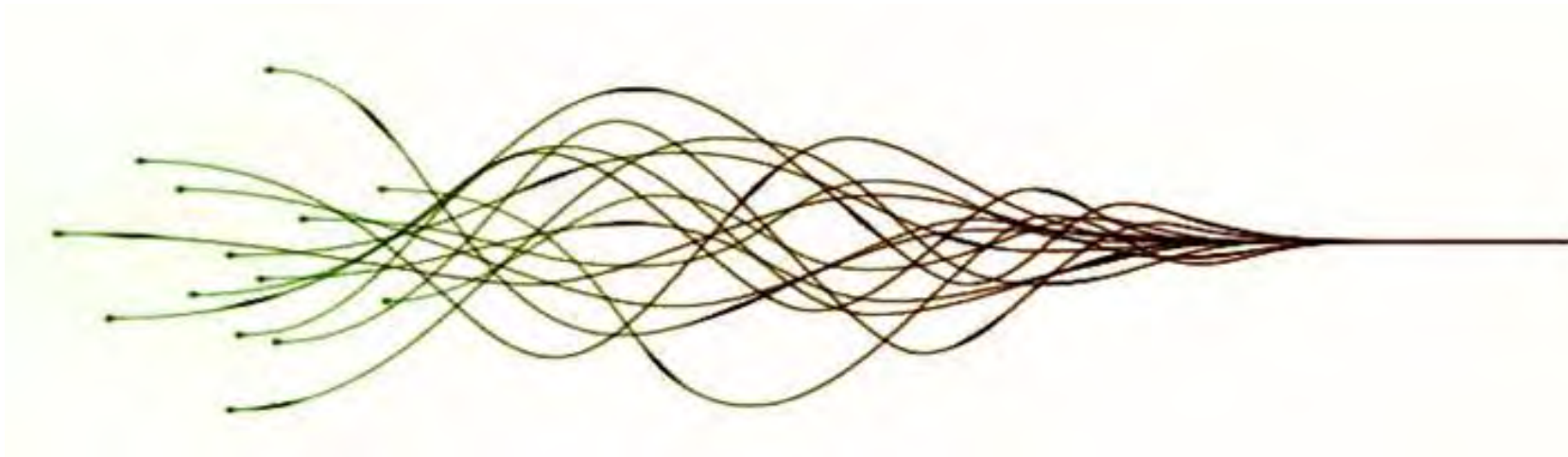
Resumen

Marco legal – nos protege a todos como ciudadanos y pacientes

Ofrecer garantías reales en la metodología de la investigación y en las fuentes de datos

Facilitar medidas técnicas y organizativas para conseguir una investigación de calidad

Compromiso en el manejo de la información clínica que facilite la investigación y en especial facilitando los proyectos de la iniciativa Europea, Española y Andaluza



dpd.sspa@juntadeandalucia.es