Confidencialidad y protección de datos en nuevos escenarios

IV Jornadas Formación CEI -IB

GOIB
CONSELLERIA SALUT I CONSUM
SERVEI SALUT ILLES BALEARS

Miguel Ángel Benito - dpd@ibsalut.es

Palma, 20 de noviembre del 2020

CONSELLERIA
SALUT I CONSUM
SERVEI SALUT
ILLES BALEARS

Contenido

1. Delegado de Protección de Datos
2. Antecedentes RGPD y LO 3/2018
3. APPS en Salud e Investigación
4. Consentimiento y protección de datos
5. Oportunidades de mejora
6. Ruegos y preguntas

1

Delegado de Protección de Datos

Delegado de Protección de Datos

https://www.ibsalut.es/es/servicio-de-salud/organizacion/organos-de-direccion/direccion-general/delegado-de-proteccion-de-datos

Funciones por áreas de trabajo

- Cumplimiento normativo
- Relación con los interesados
- Prevención
- Cooperación
- Seguridad en el tratamiento de datos personales
- Formación
- Miembro CEI-IB

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
Disposición adicional decimoséptima. Tratamientos de datos de salud.

2

Antecedentes RGPD y LO 3/2018

De dónde partimos

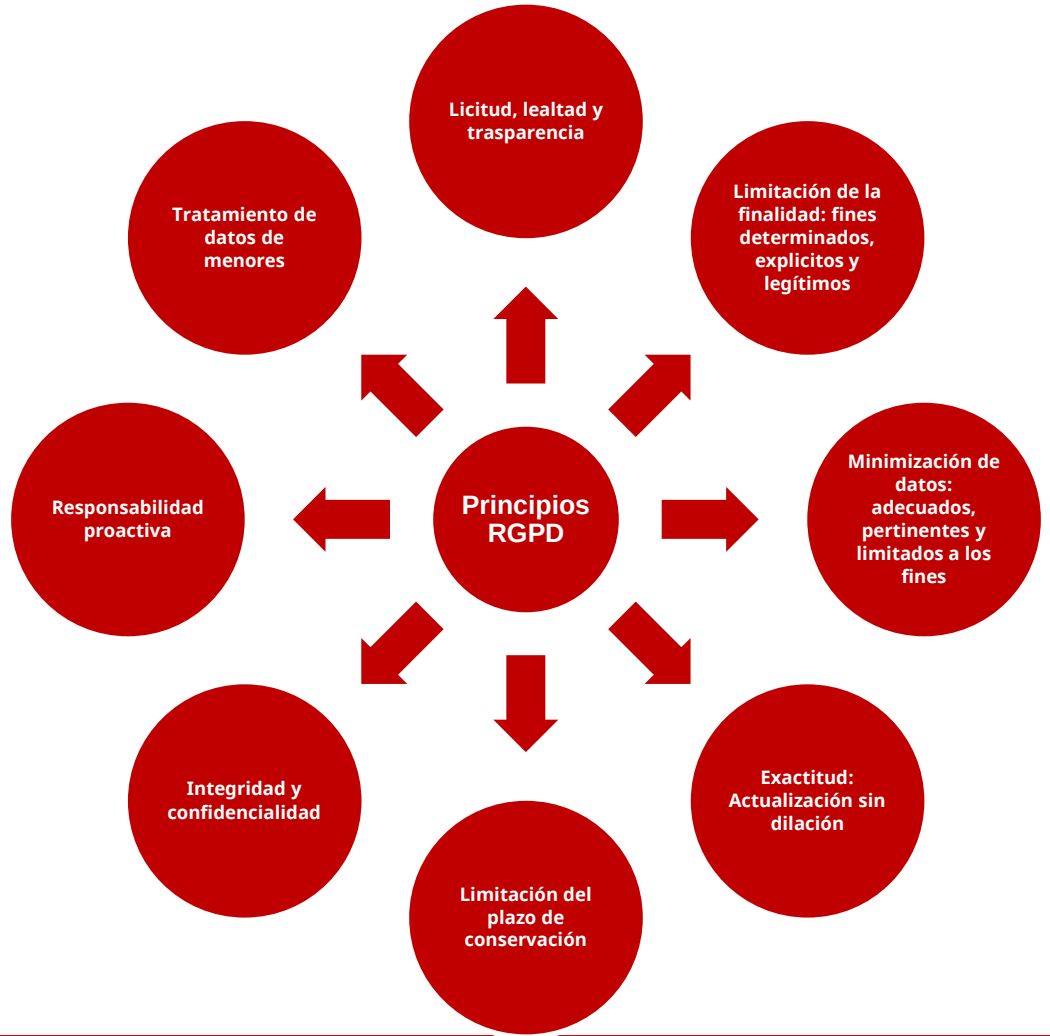
Investigación y protección de datos: ¿Qué relación tiene?

Principios RGPD

El Reglamento General de Protección de Datos (RGPD) **establece los principios relativos al tratamiento de datos de carácter personal**

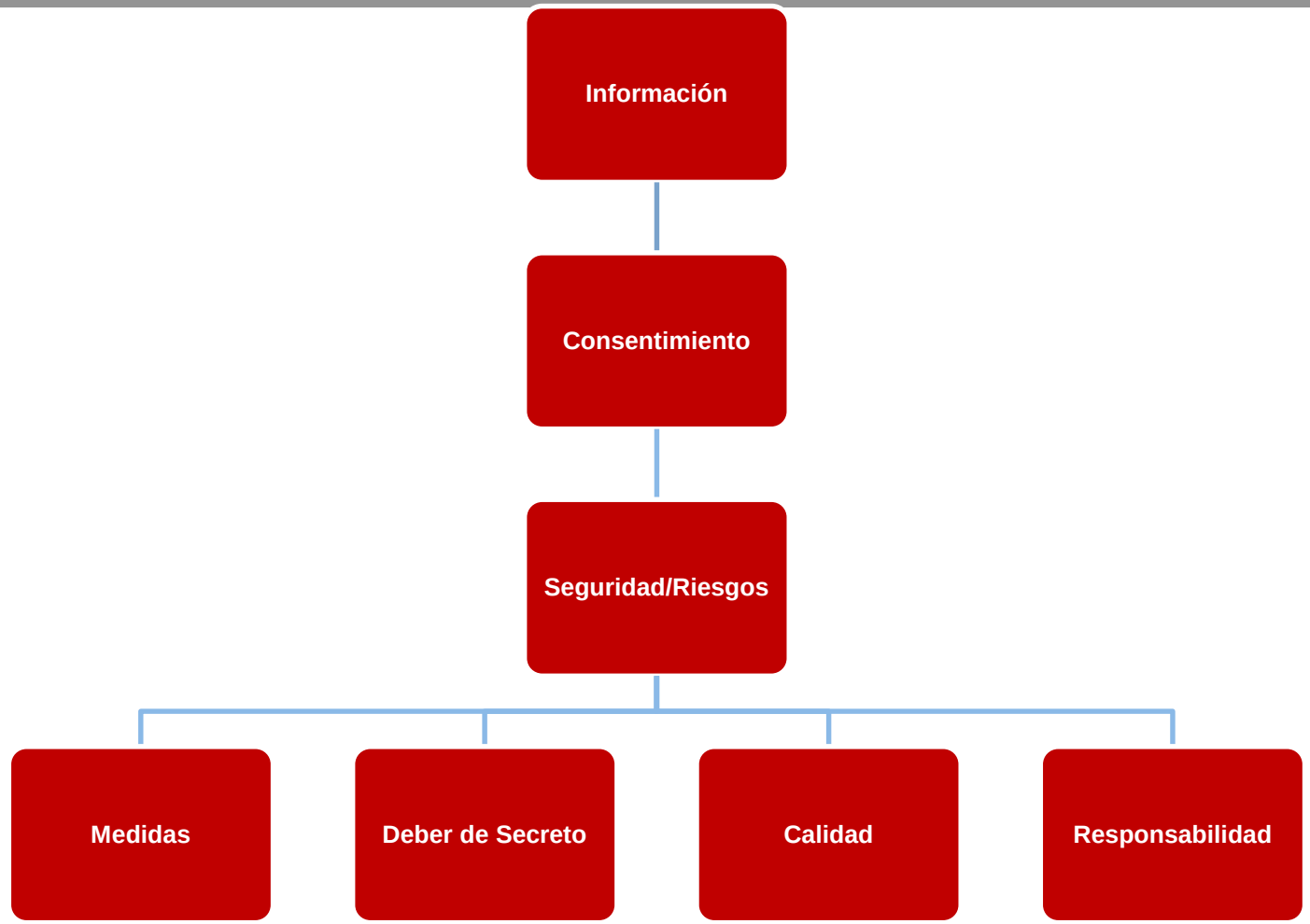
Principios RGPD

El Reglamento General de Protección de Datos (RGPD) **establece los principios relativos al tratamiento de datos de carácter personal**



Principios RGPD

Pirámides de principios



Principios RGPD

¿Por qué crees que hay que tratar los datos y sistemas de forma SEGURA, CONFIDENCIAL e ÍNTEGRA?

https://www.eldiario.es/hojaderouter/seguridad/hospitales-sanidad-segu

eldiario.es Iniciar sesión

hojaderouter.com

Realidad virtual y aumentada Robots / IA Drones Ciberseguridad Movilidad Makers IoT Ciencia y salud

CIBERSEGURIDAD

La seguridad en los hospitales españoles: tu salud y tus datos, ¿en peligro?

Los ataques contra la sanidad estadounidense han aumentado en un 125% en los últimos cinco años. Los cibercriminales hacen un lucrativo negocio con los datos de los pacientes, que pueden usarse para operar bajo una identidad falsa o estafar a las aseguradoras. Aunque en España robar la información confidencial no sea tan rentable, ¿qué mecanismos utilizan los hospitales españoles para que un atacante no pueda conseguir tus datos? Si los dispositivos médicos cada vez estarán más conectados, ¿cómo lograr que sean seguros?

09/09/2015 - 17:17h

Los ciberataques cuestan a la sanidad estadounidense 6.000 millones de dólares anualmente

Los sistemas informáticos de la sanidad estadounidense están en el punto de mira de los cibercriminales en los últimos tiempos. La compañía UCLA Health ha reconocido ser víctima de un ciberataque: los atacantes habrían podido acceder a los datos personales y médicos de 4,5 millones de pacientes porque no estaban debidamente cifrados.

No es la primera vez. **Los datos de 80 millones de personas** se vieron comprometidos a principios de año por un ataque a la **aseguradora de salud Anthem**, cuando los ciberdelincuentes consiguieron las credenciales de cinco profesionales con accesos de alto nivel al sistema. Poco después, otra compañía de seguros, Premera Blue Cross, hizo un anuncio similar, con 11 millones de pacientes afectados.

https://www.eprivacidad.es/multa-a-un-hospital-por-compartir-datos-procedentes-de-aseguradoras-privadas-con-el-servicio-de-sal

ePrivacidad® reputación en Internet SERVICIOS EN LOS MEDIOS LA FIRMA

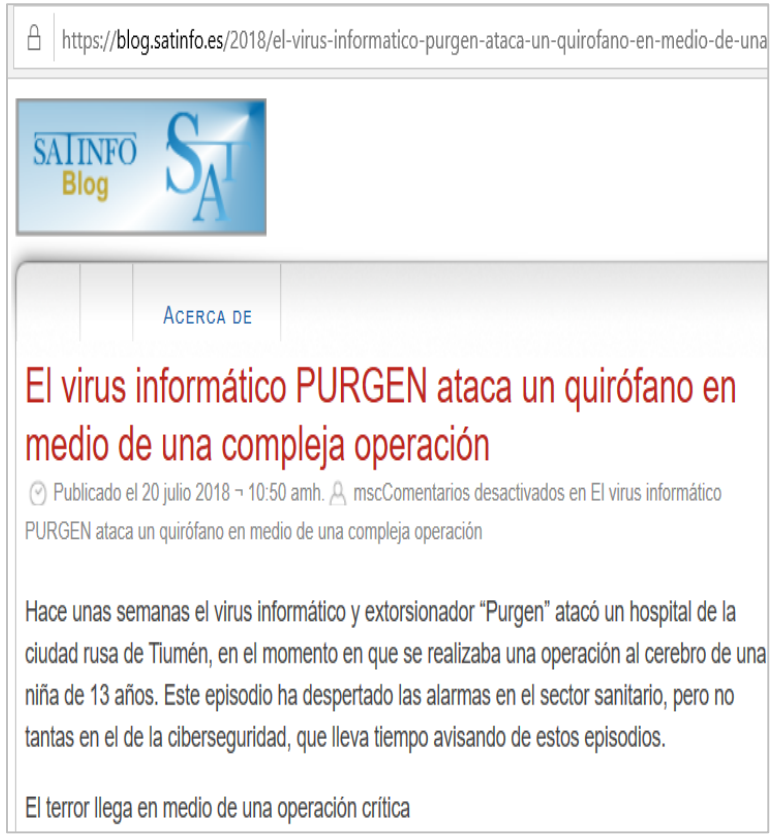
EPRIVACIDAD® - EMPRESA DE REPUTACIÓ

MULTA A UN HOSPITAL POR COMPARTIR DATOS PROCEDENTES DE ASEGURADORAS PRIVADAS CON EL SERVICIO DE SALUD GALLEGO

18 enero, 2019 por Redacción - ePrivacidad

La Agencia Española de Protección de Datos considera que un hospital privado que da servicios al servicio de sanidad pública tiene que compartir los datos de los pacientes que vienen derivados de ella, no así de los que acuden a sus instalaciones mediante aseguradora privada. La información de estos pacientes ha de ser custodiada por el hospital, pero no compartida con los profesionales de la Sanidad Pública.

Los datos de pacientes que acuden a un hospital por mediación de un seguro privado **no deben compartirse con la Seguridad Social**, resuelve la Agencia Española de Protección de Datos (AEPD). Un hospital privado gallego deberá pagar una multa de 40.000 euros tras incluir los datos de una de sus pacientes en el sistema compartido por el SERGAS (Servicio Gallego de Salud), a pesar de que esta acudía a consultas privadas.



https://blog.satinfo.es/2018/el-virus-informatico-purgen-ataca-un-quirofano-en-medio-de-una

SATINFO Blog

ACERCA DE

El virus informático PURGEN ataca un quirófano en medio de una compleja operación

Publicado el 20 julio 2018 ¬ 10:50 amh. mscComentarios desactivados en El virus informático PURGEN ataca un quirófano en medio de una compleja operación

Hace unas semanas el virus informático y extorsionador "Purgen" atacó un hospital de la ciudad rusa de Tiumén, en el momento en que se realizaba una operación al cerebro de una niña de 13 años. Este episodio ha despertado las alarmas en el sector sanitario, pero no tantas en el de la ciberseguridad, que lleva tiempo avisando de estos episodios.

El terror llega en medio de una operación crítica

Principios RGPD

¿Qué te parecería que el personal que puede acceder a tus datos los TRANSMITIERA a personal NO AUTORIZADO?

https://www.elmundo.es/elmundo/2012/05/27/andalucia_sev

ORBYT | Tienda | SuVivienda | Empleo | Coches | Moto

EL MUNDO
Líder mundial en español | Domingo 27/05/2012. Actualizado 19:35h.

Andalucía
Sevilla

España | Mundo | Europa | Op-Blogs | Deportes | Eurocopa | Economía | Vivienda | Cultur

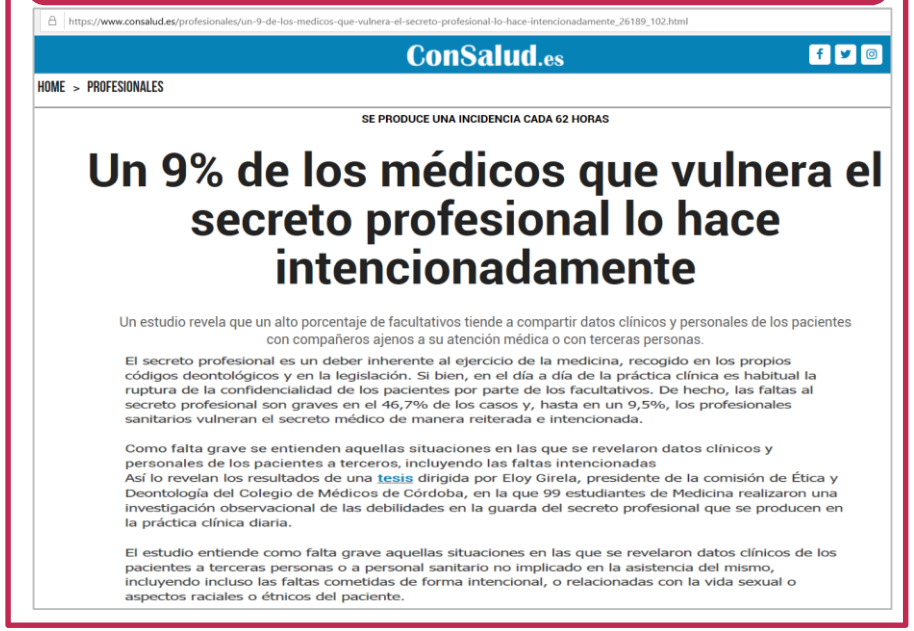
Edición ESPAÑA | Madrid | Andalucía | Baleares | Barcelona | Castilla y León | C. Valenciana

TRIBUNALES | Utilizó la documentación en un juicio

La funcionaria que divulgó el historial clínico de su ex marido ingresará en prisión

- La Audiencia de Sevilla ha ordenado el ingreso en prisión el próximo 6 de junio
- La condenada trabajó como secretaria en la subdirección médica del hospital
- Utilizó la información en un juicio contra su exmarido por malos tratos

¿Qué opinarías si estos datos fuesen tuyos o de algún familiar?



https://www.consalud.es/profesionales/un-9-de-los-medicos-que-vulnera-el-secreto-profesional-lo-hace-intencionadamente_26189_102.html

ConSalud.es

HOME > PROFESIONALES

SE PRODUCE UNA INCIDENCIA CADA 62 HORAS

Un 9% de los médicos que vulnera el secreto profesional lo hace intencionadamente

Un estudio revela que un alto porcentaje de facultativos tiende a compartir datos clínicos y personales de los pacientes con compañeros ajenos a su atención médica o con terceras personas.

El secreto profesional es un deber inherente al ejercicio de la medicina, recogido en los propios códigos deontológicos y en la legislación. Si bien, en el día a día de la práctica clínica es habitual la ruptura de la confidencialidad de los pacientes por parte de los facultativos. De hecho, las faltas al secreto profesional son graves en el 46,7% de los casos y, hasta en un 9,5%, los profesionales sanitarios vulneran el secreto médico de manera reiterada e intencionada.

Como falta grave se entienden aquellas situaciones en las que se revelaron datos clínicos y personales de los pacientes a terceros, incluyendo las faltas intencionadas
Así lo revelan los resultados de una tesis dirigida por Eloy Girela, presidente de la comisión de Ética y Deontología del Colegio de Médicos de Córdoba, en la que 99 estudiantes de Medicina realizaron una investigación observacional de las debilidades en la guarda del secreto profesional que se producen en la práctica clínica diaria.

El estudio entiende como falta grave aquellas situaciones en las que se revelaron datos clínicos de los pacientes a terceras personas o a personal sanitario no implicado en la asistencia del mismo, incluyendo incluso las faltas cometidas de forma intencional, o relacionadas con la vida sexual o aspectos raciales o étnicos del paciente.

3

APPS en Salud e Investigación

APPS en Salud e Investigación

Para garantizar la calidad, seguridad de la información, confidencialidad y privacidad de la APP se considera necesarios tener como referencia:

- **La guía sobre el uso de las tecnologías en la lucha contra el COVID19.** Agencia Española de Protección de datos. Mayo 2020.

- **Comunicado de la Comisión Europea de orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos.** Abril 2020

- **La Guía sobre la Estrategia de calidad y seguridad en las aplicaciones móviles de salud** desarrollada por la Agencia de Calidad Sanitaria de la Consejería de Salud y Familias de la Junta de Andalucía.

APPS en Salud e Investigación

EL USO DE LAS TECNOLOGÍAS EN LA LUCHA CONTRA EL COVID19. UN ANÁLISIS DE COSTES Y BENEFICIOS – AEPD MAYO 2020

Antes de implementar **soluciones tecnológicas** para enfrentarnos a la COVID-19 es imprescindible que estas se encuentren **integradas en el marco de una estrategia de medidas jurídicas y organizativas realistas, eficaces, basadas en criterios científicos, legítimas y proporcionales.**

La **proporcionalidad** se establece mediante un análisis del:

- Coste y el beneficio para la sociedad
- Los derechos y libertades del individuo

El **beneficio tendrá que medirse en función de:**

- Una menor propagación de la infección en términos globales, con la posibilidad de recuperar la libertad de acción
- La protección de la salud de los individuos.

https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf

APPS en Salud e Investigación

Tipos de aplicaciones y tratamientos

- Geolocalización de los móviles por los operadores de telecomunicaciones
- Geolocalización de los móviles a partir de redes sociales
- **Apps, webs y chatbots para auto-test o cita previa**
- Apps de información voluntaria de contagios (COVapps)
- Apps de seguimiento de contactos por bluetooth (Contact trace apps)
- Pasaportes de inmunidad
- Cámaras de infrarrojos para lecturas masivas de temperatura

Para cada una de estos tratamientos, la AEPD identifica:

- Beneficios para los ciudadanos y pacientes
- Riesgos en materia de privacidad

APPS en Salud e Investigación

- **Riesgos**
  - Una anonimización incompleta
  - Una subcontratación poco rigurosa
  - Desarrollos deficientes
  - Políticas de privacidad “opacas”
  - Un ciberataque que pusiera en manos de un tercero la información/localización de los ciudadanos
  - Prisas en poner en producción las apps y los sistemas de información
  - Ubicación de la información

APPS en Salud e Investigación

Comunicado de la Comisión Europea de orientaciones sobre las APPs móviles de apoyo a la lucha contra la pandemia de covid-19

ELEMENTOS PARA UN USO FIABLE Y RESPONSABLE DE LAS APLICACIONES

- Autoridades sanitarias nacionales (o entidades que realizan una misión que se lleva a cabo en favor del interés público en el ámbito de la salud) como responsables del tratamiento de datos
- Garantizar que la persona siga teniendo el control
- Base jurídica para el tratamiento
- Minimización de datos
- Limitar el acceso a los datos y su divulgación
- Tratamiento de los datos con fines precisos
- Establecimiento de límites estrictos al almacenamiento de datos
- Garantizar la seguridad de los datos
- Garantizar la exactitud de los datos
- Involucrar a las autoridades de protección de datos

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN

APPS en Salud e Investigación

La Guía sobre la Estrategia de calidad y seguridad en las aplicaciones móviles de salud* desarrollada por la Agencia de Calidad Sanitaria de la Consejería de Salud y Familias de la Junta de Andalucía.

Iniciada en octubre de 2012, la guía incluye recomendaciones para el diseño, uso y evaluación de aplicaciones móviles de salud dirigidas **a todos los colectivos involucrados**:

- Ciudadanía
- Profesionales sanitarios
- Proveedores de servicios sanitarios
- Desarrolladores
- …

*http://www.calidadappsalud.com/

APPS en Salud e Investigación

Las **recomendaciones** de la guía se centran en los siguientes aspectos:

- Reforzar la credibilidad de los contenidos de la APP
- Informar sobre quiénes son sus responsables
- Fuentes de información en las que se basa
- Fuentes de financiación y posibles conflictos de intereses

- Acerca de la finalidad y recogida de datos
- Tratamiento de datos personales
- Consentimiento de los usuarios
- Tratamiento de información de tipo sensible (datos de salud)
- Mecanismos de cifrado y seguridad
- Servicios en la nube
- .....

APPS en Salud e Investigación

Calidad y seguridad de la información

- **Adecuación a la audiencia**
  - **Recomendación 5.** La app de salud se adapta al tipo de destinatarios al que se dirige

- **Transparencia**
  - **Recomendación 6.** La app de salud ofrece información transparente sobre la identidad y localización de sus propietarios.
  - **Recomendación 7.** La app de salud proporciona información sobre sus fuentes de financiación, promoción y patrocinio, así como posibles conflictos de intereses.

- **Autoría**
  - **Recomendación 8.** La app de salud identifica a los autores/responsables de sus contenidos, así como su cualificación profesional.
- **Actualización de la información/revisiones**
  - **Recomendación 9.** La app de salud contiene la fecha de la última revisión realizada sobre el material publicado.
  - **Recomendación 10.** La app de salud advierte de aquellas actualizaciones que inciden o modifican funcionamientos o contenidos sobre salud o cualquier otro dato sensible.

- **Contenidos y fuentes de información**
  - **Recomendación 11.** La app de salud está basada en una o más fuentes de información fiable y toma en consideración la evidencia científica disponible.
  - **Recomendación 12.** La app de salud proporciona información concisa acerca del procedimiento utilizado para seleccionar sus contenidos.
  - **Recomendación 13.** La app de salud se sustenta en principios y valores éticos.

- **Gestión de riesgos**
  - **Recomendación 14.** Se identifican los riesgos que el manejo de la app de salud puede suponer para la seguridad del paciente.
  - **Recomendación 15.** Se analizan los riesgos y eventos adversos (o cuasi incidentes) de los que se tiene conocimiento y se ponen en marcha las actuaciones oportunas.

Confidencialidad, privacidad y protección de datos

- **Recomendación 21.** Antes de su descarga e instalación, la app de salud informa sobre qué datos del usuario se recogen y para qué fin, sobre las políticas de acceso y tratamiento de datos y acerca de posibles acuerdos comerciales con terceros.
- **Recomendación 22.** La app de salud describe de forma clara y comprensible los términos y condiciones sobre la información registrada de carácter personal.
- **Recomendación 23.** El funcionamiento de la app de salud preserva la privacidad de la información registrada, recoge consentimientos expresos del usuario y advierte de los riesgos derivados del uso de aplicaciones móviles de salud en red.
- **Recomendación 24.** Si la app de salud recoge o intercambia información de salud o cualquier otro dato especialmente sensible de sus usuarios, garantiza las medidas de seguridad correspondientes.
- **Recomendación 25.** La app de salud informa a los usuarios cuando tiene acceso a otros recursos del dispositivo, cuentas del usuario o perfiles en redes sociales.
- **Recomendación 26.** La app de salud garantiza en todo momento el derecho de acceso a la información registrada y la actualización ante cambios de su política de privacidad.
- **Recomendación 27.** La app de salud dispone de medidas para proteger a los menores de acuerdo con la legislación vigente.

APPS en Salud e Investigación

Seguridad Lógica

- **Recomendación 28.** La app de salud no presenta ningún tipo de vulnerabilidad conocida, ni incluye ningún tipo de código malicioso.
- **Recomendación 29.** La app de salud describe los procedimientos de seguridad establecidos para evitar accesos no autorizados a la información recogida de carácter personal, así como limitar el acceso a la misma por parte de terceros.
- **Recomendación 30.** La app de salud dispone de mecanismos de cifrado de información para su almacenamiento e intercambio, así como de gestión de contraseñas.
- **Recomendación 31.** La app de salud, si utiliza servicios en la nube (cloud), declara los términos y condiciones de dichos servicios y se garantizan las medidas de seguridad necesarias.

4

Consentimiento en Protección de Datos

Consentimiento en protección de datos

¿Qué es el consentimiento?

El Reglamento (UE) 2016/679 de Protección de Datos (RGPD - GDPR) establece que "**El consentimiento es toda manifestación de voluntad libre, específica, informada e inequívoca** por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen."

Consentimiento en protección de datos

¿Son necesarios datos identificativos para el objeto de la investigación?

1. ¿Qué pensaría si fueran mis datos?
2. Volver a hacerse la pregunta ¿Son necesarios datos identificativos para el objeto de la investigación?
3. Solicitar consentimiento en estudios prospectivos y retrospectivos
4. Estudios Retrospectivos, recordar el Artículo 58 de la Ley 14/2007 de Investigación:
   - El CEI puede considerar que no es necesario el consentimiento cuando no es posible solicitarlo con un esfuerzo razonable y se cumplen los criterios:

     a) Que se trate de una investigación de interés general.

     b) Que la investigación se lleve a cabo por la misma institución que solicitó el consentimiento para su obtención

     c) Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente.

     d) Que no conste una objeción expresa del paciente.

     e) Que se garantice la confidencialidad de los datos de carácter personal

Consentimiento en protección de datos

¿Cómo debe ser el consentimiento del interesado según el RGPD?

- **Consentimiento expreso.** No consentimiento tácito o por inacción del interesado
- **Consentimiento inequívoco** y que el consentimiento no implique terceros tratamientos que pudieran suponerse de forma implícita
- **Informado**. Previo a la recogida de datos, deberá informarse al interesado de todos los extremos del tratamiento (finalidad, cesiones, transferencias internacionales, ejercicio de derechos, etc.)
- **Debe ser verificable. Carga de la prueba**
- No puede pedirse de forma que condicione al interesado y no podrá pedirse en sentido negativo.

¿Cuándo debe ser explícito el consentimiento?

- Tratamiento de categorías especiales de datos (datos de salud)
- Adopción de decisiones automatizadas (big data, inteligencia artificial)
- Transferencias internacionales ¿dónde guarda los datos whatsapp, Google, Dropbox,..?

Consentimiento en protección de datos

¿Qué hay que hacer para que el consentimiento sea acreditable?

1. ¿Quién otorgó su consentimiento?
2. ¿Cuándo y cómo se otorgó el consentimiento?
3. ¿Qué información recibió la persona que consintió?. Información por capas.
    - Primera capa: información básica
    - Segunda capa: información adicional

	RESPONSABLE (del tratamiento)	FINALIDAD (del tratamiento)	LEGITIMACIÓN (del tratamiento)	DESTINATARIOS (de cesiones o transferencias)	DERECHOS (de las personas interesadas)	PROCEDENCIA (de los datos)
INFORMACIÓN BÁSICA (1º CAPA)	Identidad del responsable del tratamiento	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Base jurídica del tratamiento	Previsión o no de cesiones Previsión de Transferencias, o no, a terceros países	Referencia al ejercicio de derechos	Fuente de los datos (cuando no proceden del interesado)
INFORMACIÓN DETALLADA (2º CAPA)	• Datos de contacto del responsable • Identidad y datos de contacto del representante • Datos de contacto del Delegado de Protección de Datos.	• Descripción ampliada de los fines del tratamiento • Plazos o criterios de conservación de los datos • Decisiones automatizadas, perfiles y lógica aplicada	• Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo. • Obligación o no de facilitar datos y consecuencias de no hacerlo.	• Destinatarios o categorías de destinatarios • Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.	• Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento • Derecho a retirar el consentimiento prestado • Derecho a reclamar ante la Autoridad de control.	• Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público • Categorías de datos que se traten

https://www.esendex.es/blog/post/adapta-tu-politica-de-privacidad-al-gdpr-en-3-pasos/

Consentimiento en protección de datos

¿Cómo puedo recoger el consentimiento?

- **De manera escrita y presencial.** Sistema

- **Formularios web:** se deben tener capturas de las capas informativas con sus sellos de tiempo y evidencias correspondientes.

- **Doble verificación:** este es el caso en el que se envía al interesado un correo electrónico de verificación para confirmar su alta o suscripción. En este correo electrónico se puede insertar las capas informativas y se hacen capturas del proceso

- **Telefónica/Oral:** Esta locución debe aparecer antes de proceder a recabar los datos personales. De esta forma tendremos el consentimiento del paciente para poder tratar esos datos. **Necesidad de grabar la autorización**

- **Registro unificados de consentimientos para investigación de la CCAA (reutilización de consetimientos):**
  - Portal de presentación de consentimiento con firma electrónica cl@ve
  - Garantizar la máxima trasparencia
  - Que cada ciudadano pueda comprobar de manera electrónica
    - Los estudios de investigación que están tratando sus DCP
    - El consentimiento que prestó
  - Que cada ciudadano pueda retirar su consentimiento de manera electrónica

5

Oportunidades de Mejora

Puntos de Mejora

¿Cómo podemos mejorar?

- Formar y concienciar a los equipos de investigación, a los DPD y al personal técnico

- Desarrollo de guías de ayuda a la investigación

- Homogenizar criterios en materias como:
  - Procedimientos de recogida de consentimientos
  - Big data
  - Inteligencia Artificial
  - Apps Móviles
  - Geolocalización
  - 19/11/20. La AEPD publica una guía que analiza el uso de nuevas tecnologías en las AAPP

- Foros de Colaboración Investigadores/DPD/Personal Técnico
  - Foro de Seguridad y Protección de Datos 2021
  - Mesa “Experiencias de los Delegados de Protección de Datos en los CEI”

- Trabajar de forma conjuta

De dónde partimos

Investigación y protección de datos: ¿Qué relación tiene?

Puntos de Mejora

Referencias

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
  - https://www.boe.es/doue/2016/119/L00001-00088.pdf
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
  - **https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673**
- Comunicado de la Comisión Europea de orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos
  - **https://www.boe.es/doue/2020/124/Z01001-01009.pdf**
- La Guía sobre la Estrategia de calidad y seguridad en las aplicaciones móviles de salud
  - http://www.calidadappsalud.com/
- Guía sobre el uso de las tecnologías en la lucha contra el covid19. un análisis de costes y beneficios
  - **https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf**
- Guía sobre el uso el uso de nuevas tecnologías en las AAPP
  - https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf

6

Preguntas

Ruegos y preguntas

GOIB
CONSELLERIA SALUT I CONSUM
SERVEI SALUT ILLES BALEARS

Muchas gracias

Miguel Ángel Benito - dpd@ibsalut.es

G CONSELLERIA
O SALUT
I SERVEI SALUT
B ILLES BALEARS