DATOS DE SALUD EN DISPOSITIVOS MÓVILES Y SEGURIDAD JURÍDICA

LA SOLUCIÓN DocToDoctor©

DOC to DOCTOR

Índice

Índice de Gráficas

Índice de Tablas

I. El Problema

1. Los datos personales en el Ámbito Sanitario

El impacto de las nuevas tecnologías en el ámbito sanitario, no sólo respecto a los avances médicos, sino también en la relación médico-paciente en la prestación del servicio asistencial, implica el nacimiento de nuevos tipos de "tratamiento de datos", como es el caso de la receta electrónica, las citas médicas online, la telemedicina o la gestión digital de la historia clínica y se extiende al Big Data y la interconsulta médica a través de medios digitales.

La recogida y el tratamiento de datos de salud persiguen una finalidad muy clara: Garantizar la óptima asistencia a los pacientes, actuales y futuros. En todo Centro Asistencial Sanitario se constituye el Historial Clínico como medio de gestión de la información clínica de un paciente, donde es accesible por los distintos especialistas para la correcta atención de diagnóstico y tratamiento.

Toda la estructura de custodia de la Información de Salud se orienta hacia los desafíos de Seguridad que plantea la acumulación de grandes cantidades de información clínica de muchas personas en sistemas informáticos con muchos usuarios simultáneos. Surgen nuevos y viejos retos en esa labor:

a. Anonimato vs Precisión

A medida que los datos genómicos, moleculares y ambientales se incorporan a la práctica clínica, surge una tendencia hacia la personalización. Es una narrativa muy atractiva. A todos nos dicen que somos únicos. Pero ¿cómo se mantiene anónimo en la era de la precisión y la individualidad? ¿Es este el único valor ético en juego? Es importante considerar la forma en que se realiza la investigación clínica actual. En el estándar de oro de los ensayos de control aleatorio, la variabilidad individual se minimiza para que las manzanas se comparen con las manzanas. En la era de la precisión, esto no solo desafía el futuro de la investigación médica. También exige nuevas formas de evaluar la eficacia y la rentabilidad, al tiempo que se minimiza el sesgo. Esto es importante para la política y planificación de la salud.

b. ¿Medicina de Precisión o Salud?

Si además deseamos pasar de un paradigma de tratamiento de la salud a la prevención, debe hacerse una pregunta honesta sobre el establecimiento de objetivos. Pasando de la retórica a los resultados, los gobiernos tendrán el desafío en la próxima década de analizar sus políticas y modelos de financiación: ¿hasta qué punto fomentan el uso colectivo de los datos de salud? ¿Mejoran los tratamientos médicos o previenen la progresión a la enfermedad? Esto representa un cambio cultural en las perspectivas y expectativas de los pacientes, pero también una necesidad económica, ya que los presupuestos nacionales se ven afectados por los crecientes costos del sistema sanitario. Finalmente, también se puede reflexionar sobre los límites de los datos de salud o de la salud basada en datos, particularmente en la implementación de soluciones a problemas esencialmente sociales. La soledad, por ejemplo, es difícil de medir con datos, y aún más difícil de resolver usando datos.

El futuro de la salud y la medicina se fusionará indudablemente con la digitalización y los datos.

Esto puede parecer una evolución inevitable de los diferentes campos, pero muchos aspectos permanecen abiertos para el ajuste. Por ejemplo, ¿qué tecnologías pueden facilitar de manera sostenible el flujo de datos de salud? ¿Cómo se integrará adecuadamente el volumen creciente de datos de comportamiento con los datos clínicos? ¿Qué tipo de asociaciones crearán los gobiernos y las empresas para utilizar los datos de salud para beneficio público? Las respuestas a estas preguntas apenas están siendo clarificadas, pero una cosa es segura. La forma en que se manejan los datos de salud, así como la propiedad y el control de estos datos, condicionarán los términos para futuras negociaciones.

Las oportunidades se presentan pocas veces durante estas transiciones a gran escala. Los países europeos se encuentran en una posición única de tener altos niveles de confianza social, mentalidad colectiva orientada al bien público y una infraestructura digital y alfabetización preexistentes de registros demográficos de larga data. Mientras tanto, los ciudadanos reconocen cada vez más la necesidad de una mayor transparencia, y esto se refleja en las regulaciones del RGPD para coexistir en toda Europa. La inversión temprana en la gestión de datos de salud centrada en la persona de hoy proporcionará beneficios a las personas, sociedades y empresas de la región.

Las agendas políticas, económicas, sociales e institucionales deberán alinearse. A medida que el Consejo Europeo converge para discutir estrategias para el futuro de la región, puede comenzar explorando los méritos de la gestión de datos de salud centrados en la persona. Si no se aprovecha esta oportunidad, pronto se verán eclipsados por una situación en la que los agregadores de datos privados u otras naciones dicten las prioridades de datos para los ciudadanos europeos. Con la llegada de RGPD, se comienza a construir un marco para manejar la nueva realidad digital, a fin de crear más valor a partir de los datos al liberarlos.

c. La Custodia y el Flujo de Datos

Revisando el reporte de la **Internet Society's Online Trust Alliance** sobre incidentes de ciberseguridad de 2018, se hace evidente que los problemas de seguridad y la consecuente pérdida de información son un problema generalizado y su impacto mucho mayor al esperado.

Hay varias organizaciones que registran las violaciones de datos, en su mayoría basándose en informes públicos, aunque los resultados varían ampliamente debido a las diferentes metodologías.

Sumando todo esto, Internet Society's Online Trust Alliance estima que hubo más de 2 millones de incidentes cibernéticos en 2018, y es probable que incluso este número subestime significativamente el problema real.

Gráfica1. Cuantificación de Incidentes de Ciberseguridad en 2018

(Fuente: https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/)

d. Los Datos Personales como Producto

El desarrollo tecnológico ha permitido a gobiernos y entidades acumular una enorme cantidad de información sobre ciudadanos comunes y su comportamiento en línea, indefinidamente.

Todos los motores de búsqueda (Google, Bing, etc.) ofrecen sus servicios gratuitamente, lo que sucede igualmente con el uso de las Redes Sociales y aplicaciones de toda índole: espacio para almacenar información en la nube, música, películas, todo es gratis. Cada día que pasa tenemos menos derecho a pagar por diferentes servicios. **Axioma en boga: si no paga por un producto, es que *usted es el producto.***

El modelo de negocios es simple: ofrecer un producto o servicio online a los usuarios de manera gratuita a cambio de sus datos personales e información de comportamiento que luego será utilizado en campañas de marketing, comunicación, estadísticas, etc. en el mejor de los casos. Esos datos personales son el producto que se comercializa al mejor postor, para así optimizar el proceso de venta a través de publicidad dirigida.

Pero la voracidad por la rentabilidad ha fomentado que los métodos de recopilación de datos y el uso indiscriminado de los mismos impliquen una clara violación a la

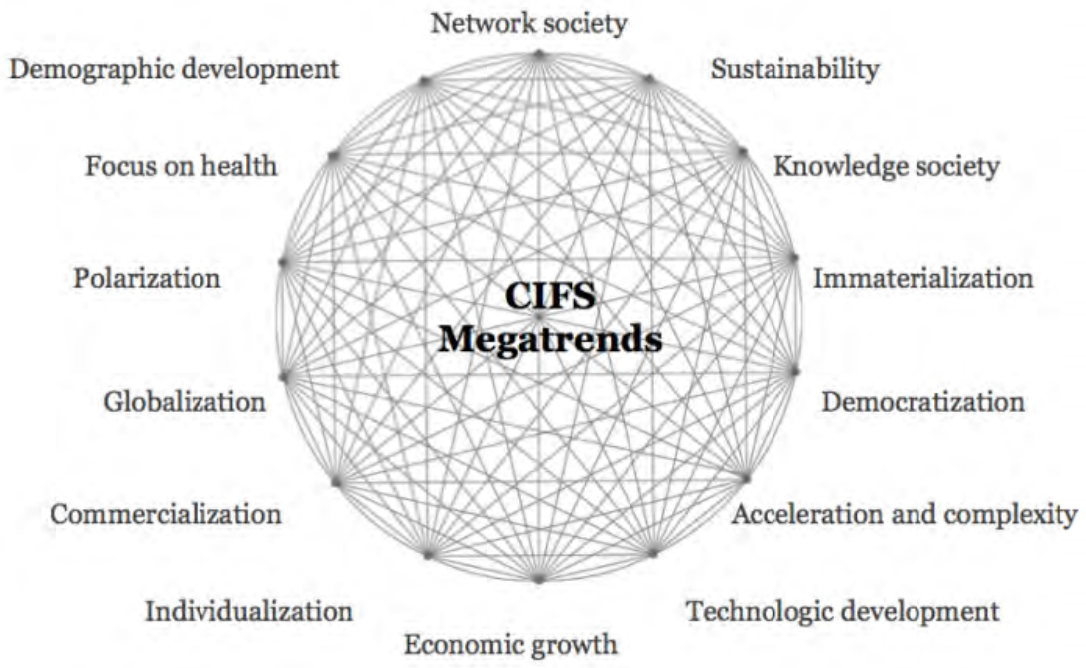
privacidad y la intimidad de las personas, que lamentablemente cuentan con pocas herramientas para cuantificar y controlar que información está siendo utilizada sin su consentimiento, y con qué fines.

El problema es tan generalizado y difundido que impacta incluso en los resultados de elecciones presidenciales de países democráticos y genera casos de discriminación política, racial, étnica o de género a escala mundial.

Los problemas de seguridad en Internet y la ubicua presencia de los *smartphones* representan hoy una seria amenaza a la privacidad de la sociedad, donde los datos personales de millones de personas en el mundo están a merced de empresas y ciber delincuentes que utilizan todos los medios disponibles para rentabilizar y explotar esos datos para su uso comercial (de forma opaca en el mejor de los casos) o directamente instrumentar delitos de muy variada índole.

2. La Relación Médico - Paciente

Todas las iniciativas mundiales sobre datos de Salud, como puede observarse en el ejemplo (Gráfica 2) de las Megatendencias según la CopenhagenInstituteforFutureStudies, están dirigidas hacia la manipulación de grandes volúmenes de datos, big data, y la interacción con otros elementos económicos. Donde no parecen dirigirse esfuerzos es en resolver el ***inicio*** de todo el proceso de recogida de información médica, la *relación médico-paciente*.



Grafica 2: Copenhagen Institute for Future Studies: Megatrends.https://cifs.dk/topics/megatrends/

Los pacientes no son un mero conjunto de datos. No son *intercambiables*, pues cada uno sobrelleva con mayor o menor penosidad su condición de salud. Los Profesionales que les atienden tampoco son intercambiables. La dinámica organizativa de instituciones grandes empuja hacia la sustitución de la relación médico-paciente por una relación paciente-Hospital. Cualquier persona, si puede elegir, decide ser atendida siempre por el mismo Facultativo y Enfermera. Las relaciones personales importan.

Hasta ahora, cualquier situación clínica especial (una lesión, una fractura, etc.) era un "*hallazgo*" personal del facultativo, un tesoro documental, que se podía conservar o no, y se usaba posteriormente para lo que el médico precisara. Ahora el RGPD aclara que forma parte indisociable de la dignidad del paciente, y con ello parte indisoluble de sí mismo.

Cuando un médico cambia de Hospital o se jubila, incluso cuando está de vacaciones, toda su experiencia profesional, su casuística, queda atrás y - casi siempre - inaccesible detrás de los mecanismos de defensa institucionales de la información.

Existen razones *legítimas* para que un profesional médico recoja *personalmente*imágenes y datos de un paciente: Investigación, Docencia,estudio reposado, correlación con resultados, recordatorios, o simplemente la creación de un álbum propio de experiencias personales y refuerzo de aprendizaje. Y también existen razones para intercambiar entre profesionales determinada información clínica a efectos de Consulta de Segunda Opinión o manejo multidisciplinar de pacientes, protegiendo el RGPD este intercambio en profesiones ligadas a Código Deontológico como es el ejercicio de la Medicina.

En un universo de aplicaciones gratuitas y cesión de datos a cambio, la crudarealidad es que la mayoría de los Profesionales Sanitarios ***utiliza su dispositivo móvil para recoger información clínica de sus pacientes***, que se entremezcla con sus datos familiares, se almacena como el resto de información del dispositivo en ***Servidores de la Nube situados en países de fuera de la UE***, generalmente USA o China, y se envía sin cortapisa alguna por ***sistemas de mensajerías manifiestamente inseguros***.

Surgió entonces la necesidad de desarrollar una App para móviles que permita a los profesionales médicos gestionar información clínica PERSONALMENTE CEDIDA por sus pacientes, porque es positivo para la asistencia individual y global a estos pacientes, cumpliendo estrictamente los requerimientos legales y técnicos que garanticen los niveles más altos en cuanto a privacidad y seguridad, aplicando los principios estipulados en el RGPD.

II. LA SOLUCIÓN DocToDoctor©

DocToDoctor© es una aplicación para dispositivos móviles (tanto para la plataforma Android, como iOS) con soporte web (https://app.doctodoctor.com/public/login) que permite a profesionales médicos capturar, archivar y compartir información clínica de manera segura, cumpliendo rigurosamente con la normativa de Protección de Datos.

Es la única herramienta online disponible que permite al profesional médico, desde su móvil y entorno informático personal, gestionar información clínica de manera legal, cumplimentando los requerimientos técnicos que salvaguardan la privacidad de sus pacientes y la seguridad de sus datos.

Seguridad	Protege bajo *cifrado* en el dispositivo los datos de Salud
Ética	Es de uso exclusivo por Facultativos Acreditados con *Verificación*
Minimización	*Minimiza* y deslocaliza los datos de identificación de pacientes, y los *seudonimiza*
Consentimiento	Facilita registrar el*Consentimiento* específico de pacientes
Protección	Protege especialmente a los menores y dependientes, con Consentimiento *adaptado*
Disociación	Utiliza Servidor de Identidades *Disociado* del Servidor de datos clínicos
Anonimización	Incorporadas herramientas de *Anonimización* de Imágenes
Transparencia	Ofrece soluciones de *Transparencia* a los pacientes sobre el destino de sus datos
Prevención	Protege on-screen las imágenes de miradas ajenas o no preparadas (*blurred*)
Privacidad	Permite *Interconsulta* de situaciones clínicas Anonimizadas con *caducidad* temporal
Comunicación	Posibilita Asistencia *Compartida* de forma Confidencial y Segura
Europeidad	Incluye sistemas de back-up cifrado sin metadatos *en nube* protegida y *situada en UE*

Tabla 01: principales características de DocToDoctor©

DocToDoctor © asiste en el trabajo de recogida de información médica potenciando la Relación Médico-Paciente. Solicita un Consentimiento personal del paciente a su médico para recoger datos de Salud asegurándose por confianza personal (trusting) que esa información será anonimizada y cifrada antes de ser compartida, y que esa distribución de los datos o fotos del paciente lo será por razones importantes como segundas opiniones, estudio posterior o investigación.

El objetivo de DocToDoctor © es integrar en la rutina profesional recoger el Consentimiento específico del paciente y facilitar tanto la toma de fotografías de procesos clínicos así como otros datos de Salud cifrados, para que el profesional pueda mantener un archivo personal de hallazgos interesantes o un registro suficientemente anonimizado de pacientes con la información necesaria para poder tomar decisiones, realizar investigación, docencia o estudio reposado y comparativo.

DocToDoctor© garantiza la custodia de dicho Consentimiento, que es necesariamente identificativo con datos personales incorporados, con cifrado potente y en un Servidor específico disociado de cualquier otro dato de Salud, y permite, en caso de ser necesario, que el Facultativo pueda demostrar la existencia de la autorización del paciente, cumpliendo plenamente los requisitos del RGPD.

Dentro de este estímulo a la vinculación entre el Médico y el paciente y sus familiares, hemos incorporado al proceso de alta en la aplicación un decálogo de instrucciones éticas para la toma de fotografías médicas, que el usuario debe leer antes de utilizar la aplicación(Tabla XX).

Normas Éticas Básicas de la Toma de Fotos Médicas

1	La imagen es propiedad exclusiva del paciente y parte de su dignidad, puede autorizarle a guardarla en todo o en parte, conservando siempre el derecho de consulta, copia, modificación o borrado.
2	El motivo para tomar una foto de un proceso médico debe ser éticamente honesto (por mejor atención al paciente, incrementar conocimiento, por docencia o investigación)
3	Debe solicitarse siempre autorización en forma de Consentimiento, del que debe conservar copia. En emergencia, debe buscarse a posteriori.
4	El encuadre debe ser solo de la lesión o zona con importancia médica. Si fuera necesario, debe tapar con ropa o sábanas el resto del paciente. Esto es mandatorio en el caso de menores.
5	No fotografiar la cara.Si es imposible, hay que anonimizarla mediante recorte (no difuminar)
6	No fotografiar marcas personales como lunares peculiares, cicatrices, tatuajes, salvo que sean el objeto de estudio, entonces el encuadre será exclusivamente de estos.
7	No se puede fotografiar los datos del paciente, ni su nombre, ni ninguno de sus datos de filiación (dirección, teléfono, fecha de nacimiento, etc.)
8	Intente que no aparezcan logotipos o imágenes que permitan identificar siquiera el Centro, Hospital o incluso país asistencia.
9	Nunca fotografiar menores sin autorización y presencia de los responsables legales.Nunca sin ropa interior.
10	Si se fotografían informes o resultados en pantalla, encuadrar sin datos de identificación del paciente o centro, o recortarlos después.

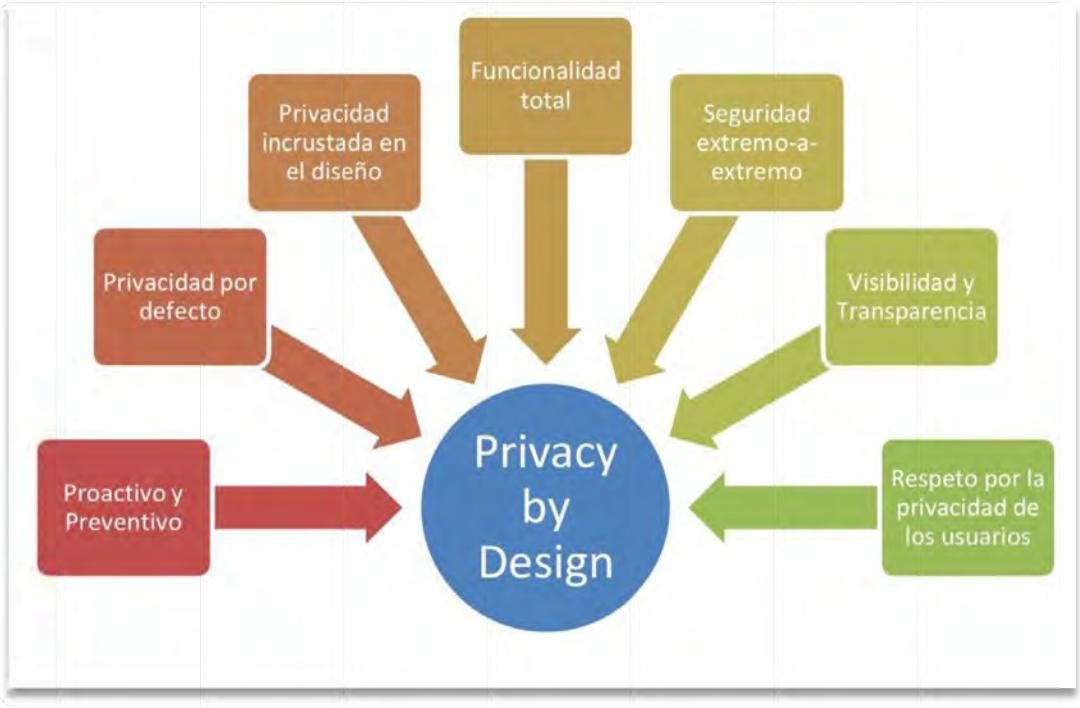
Tabla 02: Normas Éticas Básicas de la Toma de Fotos Médicas

1. "PrivacybyDesign" en DocToDoctor

DocToDoctor© es una solución para que los profesionales médicos puedan recoger en sus dispositivos móviles fotos y datos de sus pacientes de forma segura y legal.

Desde su concepción la Privacidad es el eje central de su desarrollo. Todas las decisiones de arquitectura o funcionales se han tomado en función de la seguridad y cumplimiento del RGPD, previniendo incluso la posibilidad de brechas de seguridad o mal uso de la aplicación.

A efectos prácticos, siguiendo los Principios de PrivacybyDesign, Privacidad desde el Diseño, enunciados por Ann Kavoukian y la Autoridad Holandesa de Protección de Datos en 1995 podemos enumerar, con ligero reajuste, los aspectos del funcionamiento del DocToDoctor. (Para más información: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf),



Gráfica 3: Privacy dy Design

1	Respeto por Privacidad de Usuarios	RespectofUser Privacy – Keep it User-Centric
2	Privacidad por Defecto	Privacy as the Default Setting
3	Privacidad Incrustada en el Diseño	PrivacyEmbeddedintoDesign
4	Proactividad y Preventividad	Proactive not Reactive; Preventative not Remedial
5	Funcionalidad Total	Full Functionality – Positive-Sum, not Zero-Sum
6	Seguridad Extremo-a-Extremo	End-to-End Security – Full Lifecycle Protection
7	Visibilidad y Trasparencia	Visibility and Transparency – Keep it Open

Tabla 03: PrivacybyDesign y su denominación original en inglés.

1. Respeto por la Privacidad de los Usuarios.

DocToDoctor© es una solución informática dirigida a Médicos profesionales en ejercicio con licencia legal, que se compromete desde su inicio en no ceder datos a terceros, no insertar publicidad ni practicar técnicas de spam. Los datos de los Usuarios no se usan para ninguna otra función que no sean las internas, como facturación o acreditación de identidad para acceder a sus datos.

Los datos que guardan los usuarios están cifrados y no se ejerce ningún control sobre ellos salvo el tamaño global que ocupan en Servidor.

No se solicita a sus Usuarios permisos para la cesión o el tratamiento agrupado de sus datos porque no se hace de ninguna forma.

2. Privacidad por Defecto

DocToDoctor© maneja información sensible recogida por sus Usuarios de otras personas, con las que establece una Relación Médico-Paciente que DocToDoctor© pretende potenciar y estimular. Facilita la obtención de un Consentimiento en la que el Paciente es informado del uso de la aplicación, del cuidado en que los datos y fotos sean anónimos, en su cifrado y en su custodia segura.

La Privacidad en DocToDoctor© no trabaja sobre los datos de los Usuarios, sino en la sensibilidad especial que tienen los datos que recogen los Usuarios.

Del paciente se recoge un consentimiento mediante dos posibles mecanismos:

a. Grabación de entrevistar verbal guionada donde se recoge la aceptación por el paciente de las condiciones de la recogida y almacenamiento de imágenes y datos médicos

b. Fotografía a Documentos impreso firmado, que además conserva el paciente y le permite ejercer sus derechos determinados por las condiciones ineludibles de Transparencia

Y al paciente se le solicita autorización específica para compartir sus datos con colegas, docencia, investigación o *big data*.

3. Privacidad incrustada en el Diseño

Disociación, Minimización, Desvinculación, Pseudonimización, Anonimización, Protección Cifrada, Almacenamiento Cifrado, Seguridad Reforzada y Protección de la Visión Accidental de imágenes médicas con impacto son algunos de los elementos utilizados para garantizar la Seguridad y Privacidad de los datos recogidos por los Usuarios de DocToDoctor©. Aunque luego se describen en mayor profundidad, podemos someramente indicar:

Disociación: el Consentimiento del paciente, que obligatoriamente debe contener algún dato de identidad además de su firma o su voz, se almacena en un Servidor de Identidades diferenciado lógicamente e incluso geográficamente del resto de los datos.

Minimización: los datos médicos del paciente se indexan mediante el denominado Número de Historial Clínico del centro donde es atendido, que es cifrado en el dispositivo. En si mismo, el número de Historial tiene un elevado coeficiente de K-anonimización, pues sólo tiene validez si se sabe a qué Centro pertenece el paciente, y este elemento no se recoge en modo alguno, siquiera en el Servidor de Identidades.

Desvinculación (Unlinkability):el Consentimiento no es accesible desde el Servidor de Datos, sólo si existe o no. El resto de los datos almacenados no se puede vincular a ningún paciente identificable, pues el único elemento personal es un número de Historial además cifrado en el dispositivo.

Pseudonimización: se crea un seudónimo alfanumérico para cada paciente de cada usuario, que es el dato visible en la aplicación y en el Servidor de Datos.

Anonimización: la aplicación ofrece elementos para eliminar cualquier rasgo físico identificable o dato de filiación que se haya recogido accidentalmente en una foto o documento. Guarda información anónima y elimina así mismo los metadatos de dichas fotos para que no existe datos geográficos o de dispositivo asociados, salvo que se active una función “pericial” que añade localización, fecha y hora en las fotos.

Protección Cifrada: el número de Historial es cifrado y “hasheado” en el dispositivo del Usuario, de forma que en el Servidor ese dato no es accesible, de forma que los otros datos no pueden asignarse a ningún paciente en concreto aun cuando se consiga asignar geográficamente a un Usuario con un Hospital determinado.

Almacenamiento Cifrado: tanto el Servidor de Identidades como el Servidor de Datos cuentan con altos estándares de protección cifrada de la información guardada, pero es que en el propio dispositivo del Profesional médico la información está almacenada en archivos ocultos y cifrada por clave personal.

Seguridad Reforzada: la aplicación se desbloquea por código numérico. Aunque alguien pueda coger un dispositivo ajeno y desbloquearlo, no puede acceder a la

aplicación. No se utilizan elementos biométricos porque la asistencia médica debe realizarse habitualmente con guantes y en muchas ocasiones, con mascarilla.

Protección de Visión Accidental: presenta por defecto un modo DIFUSO de navegación por fotos, *BlurredMode* en terminología informática. Las fotos, por muy cruentas que sean, están desenfocadas a menos que se inactive temporalmente por parte del Usuario.

4. Proactividad y Preventividad

Para evitar la pérdida de datos sensibles con la Privacidad de los pacientes, DocToDoctor© ha impulsado un Decálogo de Normas Éticas para la Realización de Fotografías Médicas, presentado en otra parte de esta Memoria.

La ausencia de elementos de identificación física, dirección, etcétera, es la mejor garantía contra la pérdida de datos y con ello de Privacidad.

Cuando se añade un Episodio o Paciente a un Grupo de Trabajo, para prevenir incluso el descifrado del único elemento almacenado, el Número de Historial Clínico, que es imprescindible que sea accesible a todos los miembros del grupo, se realiza mediante un una doble codificación cifrada en el dispositivo por un código transitorio, único elemento que se almacena temporalmente en el Servidor, protegiendo con ello este elemento de ataques *BruteForce* sobre los datos o que desde un usuario se pueda acceder a las claves de otros usuarios y a sus casos.

DocToDoctor© añade marcas de agua (visibles y no visibles) y tiene en desarrollo varias técnicas de esteganografía para poder realizar una Trazabilidad de la información almacenada en caso de brecha de seguridad o publicación no autorizada de la información recogida.

Este elemento de Trazabilidad es fundamental para garantizar que incluso un ataque a Servidores que acceda a la información mediante elementos de phishing permita rastrear las imágenes.

5. Funcionalidad Total

DocToDoctor© se desarrolla para ofrecer Privacidad. Es su único objetivo. No puede entrar en conflicto con ningún modelo de negocio porque los usos alternativos de la información quedan por principio desechados en aras de ofrecer Privacidad, Seguridad y Legalidad.

Los datos que almacena un Médico son también su memoria profesional. Facilitamos la anonimización para que pueda almacenarse mientras el Facultativo lo desee. En caso de que el usuario no renueve su plan de acceso tras sucesivos avisos, los datos almacenados serán destruidos al año de transcurrido el último acceso a la aplicación.

6. Seguridad Extremo a Extremo

Desde almacenar la información en un archivo cifrado y privado, no accesible por otras aplicaciones, hasta la utilización de servidores disociados y cifrados, todo el proceso de manejo de los datos en DocToDoctor© se realizan sobre la base de Seguridad.

Incluso para la operatividad de los Servidores, en el Diseño de las aplicaciones de BackEnd se ha tenido en cuenta que el personal administrativo o técnicoque tiene

acceso a ciertos datos, como por ejemplo el nombre de usuario, no puede acceder en modo alguno al Servidor de Datos, ni tampoco a los Consentimientos de los Pacientes.

7. Visibilidad y Transparencia

La dualidad del servicio que realiza DocToDoctor© tanto a Usuarios Médicos como a sus Pacientes representa un reto para garantizar la Transparencia y el ejercicio de los derechos de los pacientes.

Proteger a la vez la Intimidad del Facultativo y el Derecho de Consulta de los Pacientes se lleva a cabo al arbitrar mecanismos de fácil acceso para los Pacientes mediante la página web y una dirección de correo electrónica impresa en el Consentimiento, comunicándose al médico dicha solicitud por si él decidiera atenderla, o en caso contrario, garantizar mecanismos de identificación segura de que el paciente es quien dice ser, para luego, en un proceso manejado por el Delegado de Protección de Datos y por otro Facultativo obligado al mismo código deontológico, se muestre al paciente qué información se guarda de él o ella, y su grado de anonimización.

En caso de que un paciente solicitara la Supresión de la información que le concierne, se atenderá si no fuera completamente anónima, o en caso de que los datos se hayan incluido en alguna investigación, se comunicará tal hecho al Facultativo responsable de los datos para que actúe en consecuencia.

2. Estrategias de Diseño de Privacidad.

DocToDoctor© aplica de la siguiente forma las ocho estrategias básicas del Diseño de la Privacidad.

1	Minimizar	Seleccionar Excluir Podar	Sólo almacena número de historial clínico, cifrado Sin otros datos de localización, NHC no tiene valor Se comparten datos seudonimizados sin acceso a id
2	Ocultar	Restringir Ofuscar Disociar Agregar	BackEnd administrativo sin acceso a datos de pacientes Nº historia cifrado y hashing, inaccesible para el Servidor Doble Servidor Identidades/Datos; Supresión Metadatos No se utiliza en DocToDoctor©
3	Separar	Aislar Distribuir	Una persona puede ser paciente de dos Médicos y no hay forma posible de relacionar que tienen la misma identidad Descodificación exclusiva el Dispositivo del Nº de Historial del paciente
4	Abstraer	Sumarizar Agrupar Perturbar	No se utilizan enDocToDoctor©
5	Informar	Facilitar Explicar Notificar	Consentimiento específico y mecanismos de acceso fáciles Consentimiento claro y sencillo del objeto de la aplicación Correo electrónico y Notificaciones Push-in incorporadas
6	Controlar	Consentir Alertar Elegir Actualizar Retirar	Consentimiento en forma escrita y verbal Decálogo de Normas Éticas de Toma de Datos Funcionalidad granulada implementada Usuarios tienen acceso sin trabas a sus datos Episodios enviados caducan a las 48 horas.
7	Cumplir	Definir Mantener Defender	Acceso a datos de Pacientes cuando estos lo solicitan Implantadas medidas técnicas para impedir acceso externo Chequeo diario de accesos
8	Demostrar	Registrar Auditar Informar	Existe registro de decisiones de desarrollo y servicio En desarrollo Consulta previa realizada a la AEPD sobre Compartir(*)

Tabla 04: Estrategias de Diseño de Privacidad.

(*) [Addenda 2: justificante de la pregunta realizada a la AEPD sobre la función Compartir, específicamente, sobre Compartir en Grupo.

3. Objetivos de Privacidad y Seguridad

Los tres nuevos objetivos de Protección Específicos de la Privacidad que deben garantizarse en la ejecución de un proyecto actual de tratamiento de Datos se encuentran adecuadamente desarrollados en DocToDoctor©. De esta forma es demostrable, como se verá más abajo en sus Elementos de Seguridad, que la aplicación cumple con:

1. **Desvinculación (Unlinkability):** el mecanismo de cifrado en el dispositivo del único elemento de identificación real, unido a la deslocalización geográfica de los metadatos, así como al seudonimización del usuario, hace muy difícil que pueda vincularse los datos almacenados en DocToDoctor© con ningún sujeto específico. Este hace muy difícil, por otro lado, llevar a cabo los otros dos aspectos de este apartado que vienen a continuación.

2. **Transparencia (Transparency)**: en el siguiente capítulo se comenta por extenso este tema, pero puede comentarse aquí que DocToDoctor© desarrolla los principios de Lealtad tanto a los Usuarios como a los pacientes originarios cuyos datos almacenan aquellos, pues el Consentimiento que se solicita al Paciente especifica los distintos tratamientos a que serán eventualmente sometidos sus datos.

3. **Control (Intervenability)**: se establecen mecanismos dedicados a que el paciente pueda tener acceso a su información. De cualquier manera, y dada la naturaleza de los datos guardados, este sistema de Consulta y Rectificación o Supresión no se hará nunca por medio de sistemas automáticos o por acceso directo del paciente a sus datos. En todo momento el acceso estará guiado por el Delegado de Protección de Datos, pero el acceso a la información almacenada, si fuera necesario para certificar su anonimato, por ejemplo, sólo será realizado por personal médico sujeto a código deontológico, y no por personal administrativo.

4. Trasparencia vs Anonimización

Uno de los requisitos a que obliga el RGPD es el de *Transparencia***:** que los usuarios pueden conocer en todo momento qué información de ellos se guarda y qué uso se da a esa información.

Los Usuarios de DocToDoctor© son los Facultativos Médicos que utilizan la aplicación, y los datos que se mantienen de estos usuarios no se ceden a terceros, al igual que no se permite realizar spam o publicidad, ni desde el programa ni a las direcciones de correo. En el Addendum 1 se transcribe el registro de datos de tratamiento de la aplicación.

Si un paciente lo solicitase, o una auditoria de Protección de Datos, o una instrucción judicial, o si por cualquier otro motivo el Médico necesita demostrar la existencia del Consentimiento del paciente, los usuarios disponen de una dirección mail específica (user@doctodoctor.com) y un teléfono gratuito (902955531).

DocToDoctor© propone ir un paso más allá, y establece un mecanismo completamente novedoso que concede a los pacientes la posibilidad de ejercer sus derechos acorde a la transparencia, interfiriendo lo menos posible en la actividad profesional de los Médicos usuarios.

DocToDoctor© sirve de enlace entre Facultativos y Pacientes, y permite a estos últimos conocer qué información se guarda de ellos, confirmar que se encuentra completamente anonimizada, y si ha sido compartida con otros Profesionales.

Pero al practicar la minimización de datos al extremo, y la seudonimización, *DocToDoctor© no conoce* la identidad de los pacientes. Ésta se encuentra únicamente formando parte del Consentimiento bien en forma de archivo de audio, bien en forma de fotografía, cifrados en un servidor unidireccional que denominamos Servidor de Identidades. Si no existe Consentimiento, de cualquier forma, la información no ha podido ser compartida a otros usuarios o en grupos de trabajo.

Todo el proceso de Transparencia debe realizarse por operadores humanos, bajo el control del Delegado de Protección de Datos deDocToDoctor©, siendo imposible la automatización si se quiere mantener los altos requerimientos de Seguridad que DocToDoctor©procura.

DocToDoctor© brinda dos formas de ejecutar Transparencia asociada a máxima Protección, completando una potente característica de Control (Intervenability).

a. El consentimiento impreso porta un código QR con datos cifrados que nos permiten identificar el número de documento y localizarlo en el Servidor de Identidades (ver más abajo).

b. En caso de consentimiento verbal el médico usuario debe informarnos del seudónimo del paciente. DocToDoctor© intermedia cuando un paciente solicita información, y media frente al usuario para lograr la información necesaria y mostrarla al paciente.

Una vez confirmada la identidad del paciente por mecanismos seguros que incluyen la aportación de un documento de identidad con foto y de una fotografía del paciente con dicho documento (datos que inmediatamente son destruidos y no almacenados), y con el conocimiento por parte del Facultativo, se certifica al paciente que sus datos están anonimizados y no pueden ser reconocibles por ningún sistema de Des-identificación. Asimismo, se le informará si alguno de sus datos o imágenes ha sido compartido.

Si el paciente tuviera dudas, solicitará a un Comité Ético formado por médicos en ejercicio, que revisará la información guardada y confirmará la anonimización absoluta. El personal administrativo e informático convertirá el cifrado interno del Servidor en un nuevo archivo cifrado, cuya clave no conocerán, de forma que no puede acceder a los datos almacenados, además de existir una *cláusula de no acceso* en sus contratos (además de la de Confidencialidad habitual).

El paciente podrá acceder a una imagen de baja resolución de aquellas fotos suyas guardadas, aun así cifrada, con mecanismos de protección de aspectos cruentos o desagradables.

El paciente que sabe que su médico ha utilizado nuestra aplicación para guardar información suya, puede solicitar el destino de esa información iniciando el procedimiento en la página web.

Deberá ofrecer pruebas fidedignas de su identidad, y una fotografía del Consentimiento impreso que le fue entregada, o la fecha aproximada en que cree que otorgó el Consentimiento escrito. En este último caso su médico es el que debe informarnos de ciertos datos relativos a poder encontrar su información.

DocToDoctor© garantiza Anonimidad y Seguridad, pero a la vez Transparencia a un doble nivel, para los Usuarios y para los Pacientes que permiten que se almacenen sus datos de Salud.

III. ELEMENTOS DE SEGURIDAD INCORPORADOS

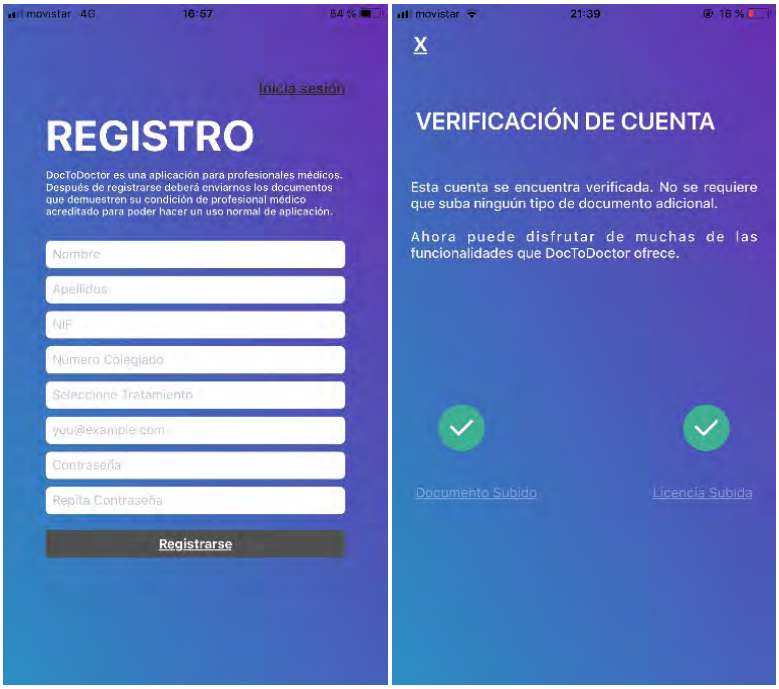
DocToDoctor© integra múltiples niveles de protección de la información de datos de Salud de los pacientes, así como de los Usuarios.

	Función	Características	Datos
1	Registro	Incluye datos personales, profesionales y de pago	personales
2	Usuario	Dirección e-mail	email
3	Acreditación	Debe verificarse la Licencia Profesional para ejercer	licencia
4	Aceptación	Política de Protección de Datos y Términos y Condiciones	Selector on/off
5	Clave	Código personal para cifrado de datos en dispositivo	código numérico
6	Bloqueo	Bloqueo de la aplicación y acceso a datos cifrados	código numérico
7	Recuperación	Datos bloqueados requieren identificación personal	foto con Doc ID
8	Seudonimización	Se crea seudónimo y todos los datos se indexan con este	Iniciales: user+cifra

Tabla 05: Medidas de Seguridad de DocToDoctor©1-8

1. DocToDoctor©obliga a realizar un Registro que incluye como datos el nombre y apellidos del Usuario, dirección mail, su número de documento de identidad, número de licencia profesional, y tratamiento profesional (más abajo se señala el destino de la información suministrada).

2. El nombre de usuario será la dirección e-mail del Usuario, que deberá confirmar su existencia real como mecanismo de acreditación en dos fases automático.

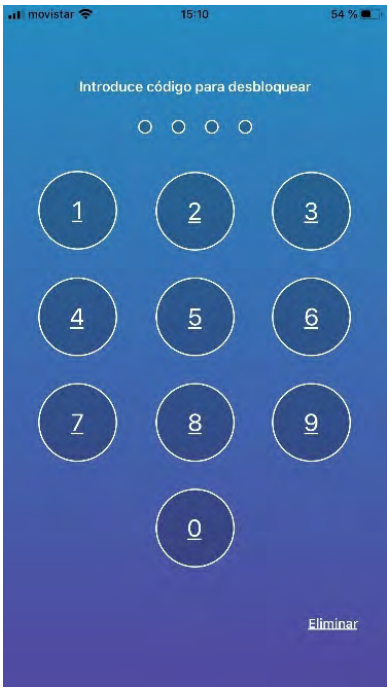


Gráfica 4: pantalla de Registro (izquierda) y confirmación de Verificación (derecha)

3. El programa funciona de forma limitada hasta que no se lleve a cabo la Verificación de la pertenencia a la Profesión Médica legalmente acreditada, con obligatoriedad de incorporar imagen de documentación personal con nombre y fotografía y licencia médica habilitante (en España número de colegiado), que se confirma en los países donde existe sistema informático, como mantienen el Colegio Oficial de Médicos o el British Medical Council. El sistema de verificación es humano, no automatizado. Esta medida acredita la pertenencia a colectivo sujeto a Código Deontológico, con las salvedades que el RGPD otorga (más abajo se señala el destino de la información suministrada).

4. En el primer uso de la aplicación el Usuario debe aceptar, además de Política de Protección de Datos (https://doctodoctor.com/es/politica-de-proteccion-de-datos/) y los Términos y Condiciones (https://doctodoctor.com/es/terminos-y-condiciones/), y leer las Normas Éticas de la Toma de Fotografías en Medicina mostradas previamente.

5. El Usuario finaliza su activación introduciendo un código personal numérico en su terminal que no se guardará en Servidor.La clave personal, al ser un código numérico presenta ciertas limitaciones, pero se ve fortalecido cuando aplicamos una derivación de clave utilizando el estándar PKCS#5. Este estándar basa su derivación de claves en técnicas de “Salting”, para añadir aleatoriedad a la clave; y “Key Stretching”, para añadir dificultad computacional a la propia derivación de la clave. Esto hace que la clave que se genera para el cifrado sea fuerte frente a ataques de “de diccionario” (es decir, probando distintas combinaciones de forma automática) o “fuerza bruta” (es decir, probando todas las posibles combinaciones hasta dar con la contraseña oportuna).



Grafica 5: Pantalla de acceso por PIN numérico

6. Esta clave personal será necesaria para desbloquear la aplicación si no se ha estado utilizando en los últimos diez minutos, y para desbloquear funciones específicas dentro de la app. La introducción de 4 claves erróneas bloqueará la app durante una hora, y un segundo intento de 4 veces con clave errónea llevará al bloqueo completo de la app. Nótese que el Servidor no guarda la clave.

7. Para poder acceder a la información almacenada en Servidor el Usuario deberá volverse a acreditar subiendo la imagen de la documentación con foto, esta vez mostrándola junto a su propia cara. Como se verá más abajo, cierta información no podrá ser recuperada nunca.

8. El Usuario recibe del sistema un Seudónimo consistente en las iniciales de su nombre y un número correlativo (i.e. ME18) que servirá posteriormente como base para la seudonimización de los pacientes.

	Función	Características	Datos
9	Disociación	Servidor de Identidades diferenciado y cifrado	usuario y pago
10	Anonimización	Nº Historial cifrado en dispositivo por clave personal	hash paciente
11	Seudonimización	Identidad visible de paciente seudónimo usuario+cifra	user+cifra
12	Consentimiento	1er paso creación de Episodio. a) Documento firmado	Foto
13		b) Grabación paciente	Vox paciente
14	Transparencia	Consentimiento impreso porta código QR y mail acceso	QR + email
15	Supresión	Mecanismo de contacto con DelegadoProt. Datos	eliminación
16	Cifrado	Consentimiento no es accesible en dispositivo	nombre real pac

Tabla 06: Medidas de Seguridad de DocToDoctor©9-16

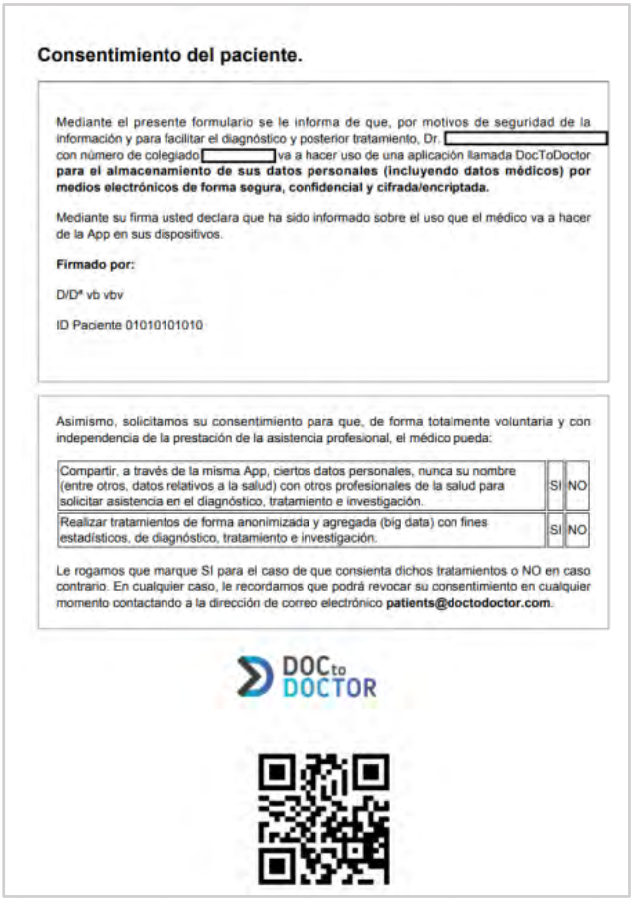
9. Todos los datos del Usuario mostrados previamente, así como los posibles datos de facturación y para la pasarela de pago, se guardarán sin geolocalización en un Servidor de Identidades físicamente independiente y actualmente situado en Francia, cifrado mediante OpenSSL y el algoritmo AES-256-CBC.

10. Un/a Usuario/a que quiera registrar información de un paciente, sea una fotografía o cualquier otra información debe crear un Episodio Clínico. El único dato de filiación real de un/una paciente que se ha previsto en la App es la introducción del Número de Historial Clínico del paciente en el Centro en que es atendido, sea éste un gran Hospital o una pequeña Consulta privada. Este número se cifra en el propio dispositivo mediante la clave personal, y el Servidor sólo registra el hash resultante. Sin datos de localización geográfica, además, este número presenta un factor de K-anonimización muy elevado, pues podría corresponder a cualquier centro hospitalario. Por si se consigue asignar localización geográfica es por lo que además se cifra con la clave personal.

11. Al introducir el número de historial se genera un seudónimo basado en el seudónimo del Usuario asociado a un contador de caso específico, denominándose al episodio con la suma de ambos (i.e. ME18-0001). Si el usuario no introduce ningún número de historial, se genera igualmente un seudónimo con contador correlativo.

12. Inmediatamente a la introducción del número de historial y a la creación del seudónimo, la app ofrece un mecanismo para captar un Consentimiento Específico de los pacientes, autorizando a la recogida anonimizada de datos y fotos de su situación clínica, y la posibilidad de compartir esa información con otros Profesionales de la Salud obligados a Código Deontológico.

13. Este Consentimiento informado puede recogerse en la propia app de dos formas:
    a) Como fotografía de consentimiento escrito, generado por la propia aplicación o desde la cuenta web del Usuario. Este Consentimiento cumple todos los requisitos sugeridos por el Documento: https://www.aepd.es/media/guias/guia-modelo-clausula-informativa.pdf



Consentimiento del paciente.

Mediante el presente formulario se le informa de que, por motivos de seguridad de la información y para facilitar el diagnóstico y posterior tratamiento, Dr. [redacted] con número de colegiado [redacted] va a hacer uso de una aplicación llamada DocToDoctor **para el almacenamiento de sus datos personales (incluyendo datos médicos) por medios electrónicos de forma segura, confidencial y cifrada/encriptada.**

Mediante su firma usted declara que ha sido informado sobre el uso que el médico va a hacer de la App en sus dispositivos.

Firmado por:

D/Dª vb vbv

ID Paciente 01010101010

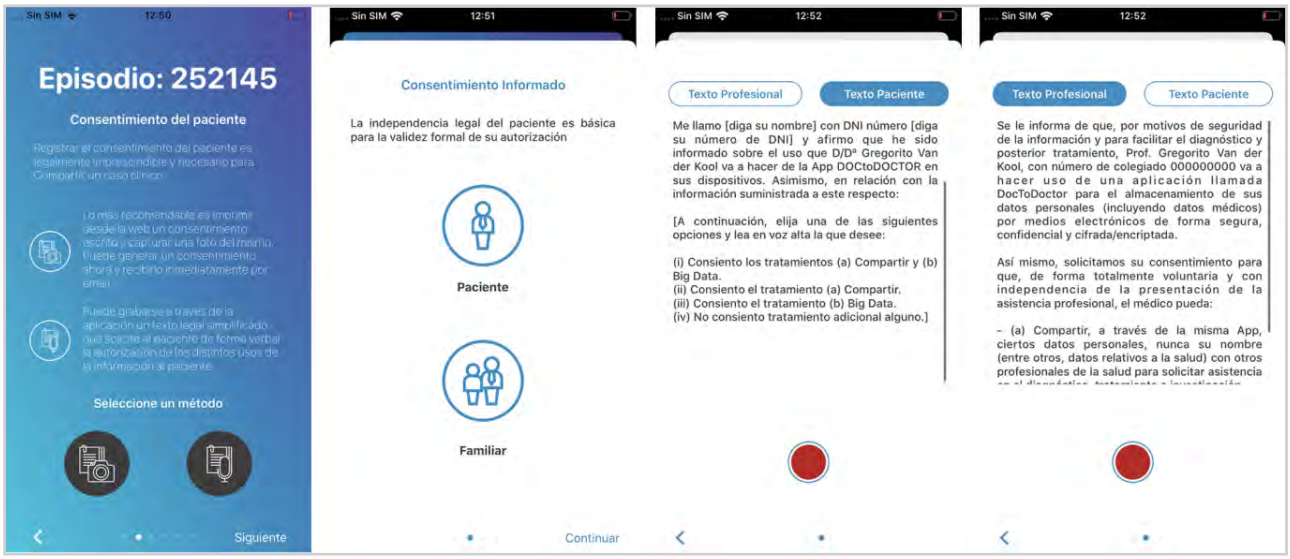
Asimismo, solicitamos su consentimiento para que, de forma totalmente voluntaria y con independencia de la prestación de la asistencia profesional, el médico pueda:

Compartir, a través de la misma App, ciertos datos personales, nunca su nombre (entre otros, datos relativos a la salud) con otros profesionales de la salud para solicitar asistencia en el diagnóstico, tratamiento e investigación.	SI	NO
Realizar tratamientos de forma anonimizada y agregada (big data) con fines estadísticos, de diagnóstico, tratamiento e investigación.	SI	NO

Le rogamos que marque SI para el caso de que consienta dichos tratamientos o NO en caso contrario. En cualquier caso, le recordamos que podrá revocar su consentimiento en cualquier momento contactando a la dirección de correo electrónico **patients@doctodoctor.com**.

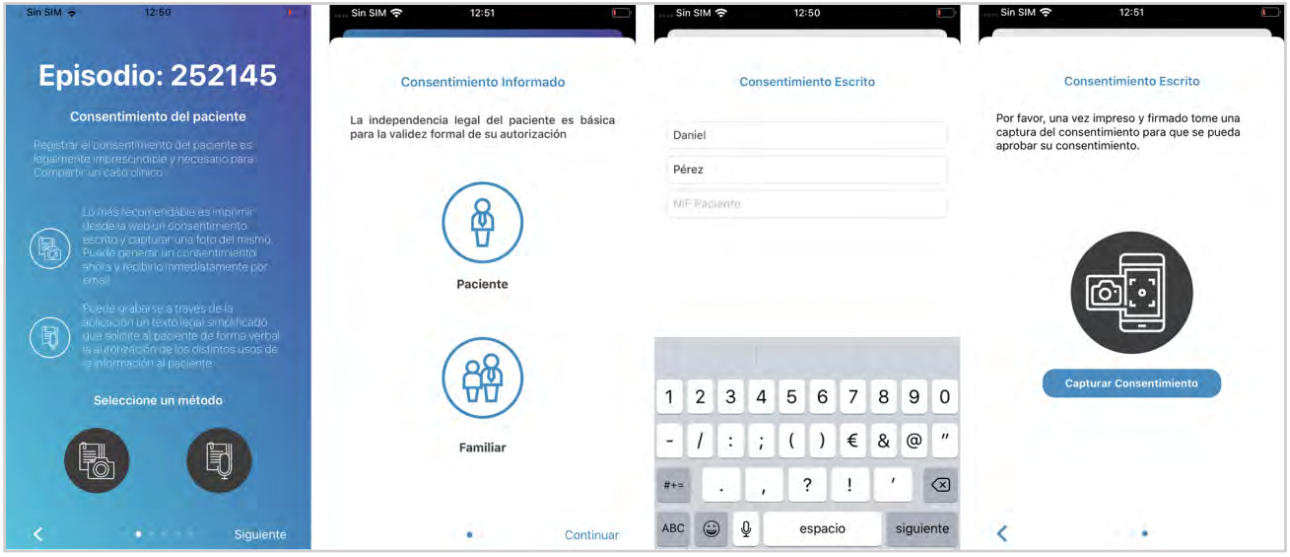
Gráfico 6: muestra real (anonimizada) de Consentimiento Impreso

    b) Como grabación de audio de Consentimiento Verbal, en el que el Usuario explica la naturaleza del Consentimiento y pregunta por la autorización específica de diversos ítems. Cumple las mismas recomendaciones, procurando un lenguaje sencillo y comprensible por el Paciente.



Gráfica7: ejemplo anonimizado de pantallas de Consentimiento Verbal

14. El Consentimiento escrito o impreso lo conserva el paciente. En él consta una dirección mail en la que el Paciente, aportando copia de dicho consentimiento (porta un código QR) y un documento de identidad con foto, puede ejercer sus derechos de Consulta al Delegado de Protección de Datos, pudiendo exigir la verificación de la anonimidad de los datos recogidos en su nombre (que realiza un Facultativo registrado y no el Delegado) y el destino de dichos datos si han sido compartidos (se ofrece número de profesionales que lo han recibido, no sus nombres).



Gráfica 8: ejemplo de solicitud de generación de Consentimiento Impreso

15. En caso de que decida ejercer su derecho a la Supresión, el Delegado de Protección de Datos se pondrá en contacto con el Facultativo para informarle del hecho y procederá a su eliminación.

16. Independientemente del tipo de Consentimiento, como contiene necesariamente el nombre del paciente y algún otro dato de identificación, es Cifradomediante el algoritmo AES-256-CBCinmediatamente en el Dispositivo con clave generada en el dispositivo y desconocida por el Administrador del Servidor,trasparente para el Usuario pero inaccesible. Este Consentimiento es archivado aparte en la memoria del dispositivo, y posteriormente en el Servidor de Identidades bajo el Seudónimo del paciente, pero sólo puede ser accesible por el Administrador del Servidor.

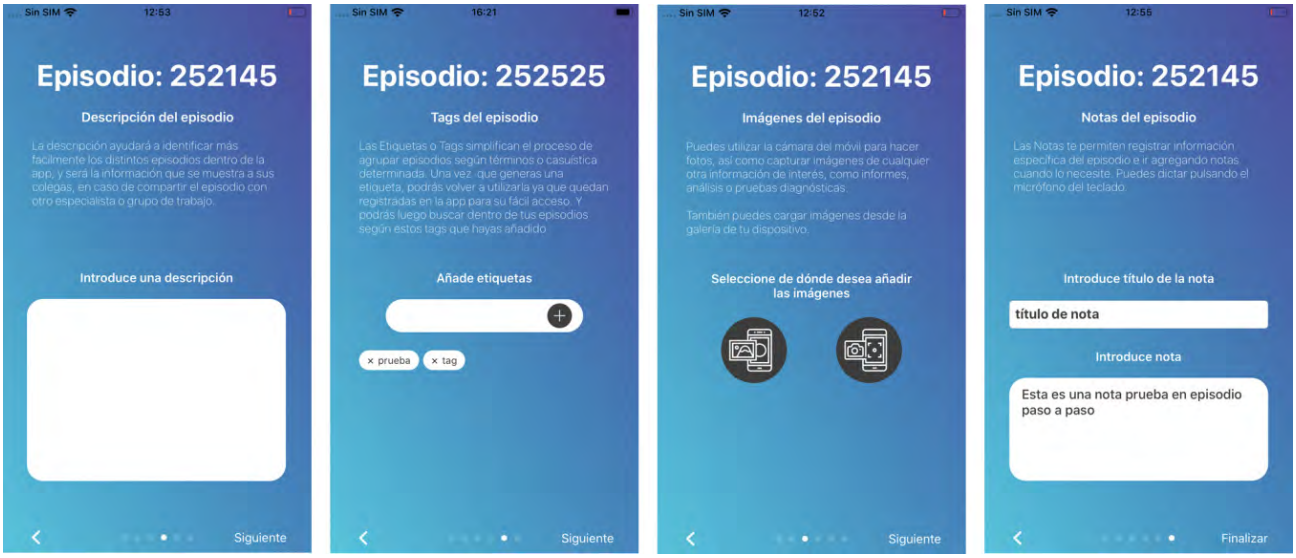
	Función	Características	Datos
17	Unidireccional	Servidor de Identidades lectura no accesible desde la app	Disociación absol.
18	Complemento	Descripción, Notas, Etiquetas, Fotos del caso clínico	Clínicos específicos
19	Disociación (2)	Servidor de Datos separado indexado por seudónimo	Acceso Web
20	Confirmación	Acreditación de doble paso para acceso web	Doble paso
21	Intromisión	Vista borrosa de Atlas para evitar miradas externas	Blurredvision
22	Compartir	Fotos o Episodios anónimos compartidos por 48 horas	Clínicos anónimos
23	Grupos	Acceso múltiple con acceso a NH real por índice virtual	key-chain
24	Trazabilidad	Marcas de agua / Esteganografía /Metados cifrados	Identificador copia

Tabla 07: Medidas de Seguridad de DocToDoctor© 17-24

17. El Servidor de Identidades presenta acceso unidireccional, sirviendo sólo para almacenar los datos de Usuario y el Consentimiento del Paciente, sin otra ninguna relación de lectura, lógica ni física, accesible por el dispositivo móvil o desde el Servidor de Datos. De esta forma se ofrece una Disociación absoluta de los datos.

18. Una vez creado el seudónimo, el Usuario puede guardar cuatro tipos de información del paciente:
    a) Descripción, un somero resumen del caso clínico que sirva de recordatorio en el futuro

b) Etiquetas-Tags, campos de textos cortos que describan y permitan la indexación de la información
c) Fotos tomadas desde la propia app, que no las almacena en el rollo o carrete habitual del dispositivo, o importándolas de éste y permitiendo su borrado del original.
d) Notas Clínicas, documentos de texto que sirven para reflejar eventos sucesivos en el devenir clínico del Paciente.

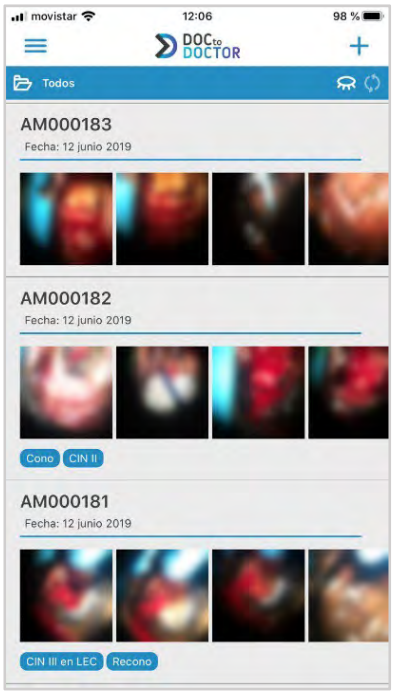


Gráfica 9: ejemplo de Nuevo Episodio (paso a Paso)

19. Todos estos elementos son cifrados mediante OpenSSL y el algoritmo AES-256-CBC y almacenados previa sincronización en un Servidor de Datos diferenciado localizado en Europa, con transferencia de datos protegida mediante SSL.Este Servidor permite mantener no sólo una copia de seguridad, sino un registro completo de los casos administrados por el Profesional, que pueden estar contenidos en el móvil o haber sido borrados por espacio.

20. El acceso a la información de pacientes almacenada en la web precisará en su momento de la acreditación de doble paso.

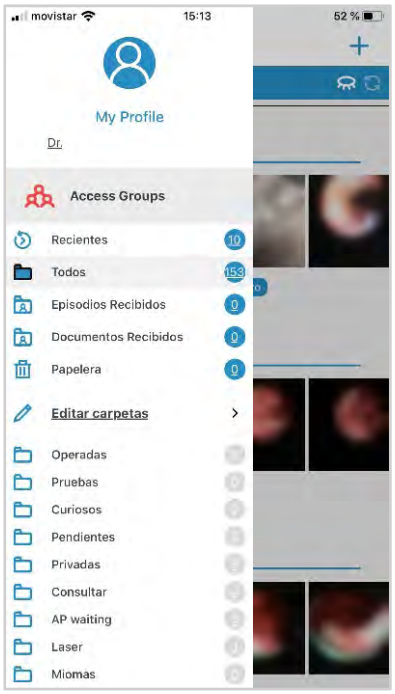
21. Implementación por defecto de modo de visión “Blurred”, con las imágenes clínicas difuminadas para ahorrar la visión de elementos sensibles por parte de profanos.



Gráfica 10: capturade pantalla real de visión difuminada o Blurred

22. Pueden realizarse Consulta Rápidas entre profesionales mediante dos mecanismos:
    a) Envío de fotografías, sin nombre ni metadatos. Desaparecen del dispositivo del receptor a las 48 horas.
    b) Envío de casos completos, con seudónimo, sin posibilidad del receptor de conocer el número de identificación real del paciente, y que también desaparecen a las 48 horas

23. Creación de Grupos de Usuarios que comparten Episodios Clínicos, permitiendo el seguimiento clínico por diversos profesionales. Para eliminar el riesgo de pérdida de seudonimización, se ha implementado un mecanismo de key-chain enmascarado cifrado que permite a cada usuario generar su propia clave de cifrado para cada episodio, sin posibilidad de desentrañar las claves ajenas.



Gráfica 11: menú acceso a Grupos de Trabajo

24. Inserción de Marcas de Agua y otras medidas de Esteganografía que permitan la trazabilidad de las imágenes guardadas en la aplicación, con contador de copias y otros datos cifrados.

Respuesta a Brechas de Seguridad

El RGPD acota tiempos precisos de respuesta en caso de Brecha de Seguridad. DocToDoctor y Molinapps han implementado diversas estrategias de resolución de conflictos de Seguridad. Podríamos diferenciarlas dependiendo del extremo en que se producen:

1. Desde el Usuario

En el caso de que un Usuario estime que su contraseña ha sido robada o que ha perdido el teléfono móvil, o cualquier otro evento en su extremo que podría conseguir el acceso a datos de sus pacientes, DocToDoctor ofrece tres elementos de respuesta rápida:

a) Sala de Chat desde la página de Web. Durante 16 horas al día existe operador accesible en sala de chat de fácil acceso en www.doctodoctor.com
b) Dirección de correo electrónico específica (user@doctodoctor.com)
c) Teléfono gratuito 902955531

2. En el Servidor

La Disociación entre Servidor de Identidades y Servidor de Datos implica invertir un gran esfuerzo para acceder a dos sistemas separados, y enfrentarse a claves de cifrado complejas. En el caso de que nuestros Operadores encuentren un acceso no autorizado a datos de un Usuario o de muchos, el Protocolo previsto contempla:

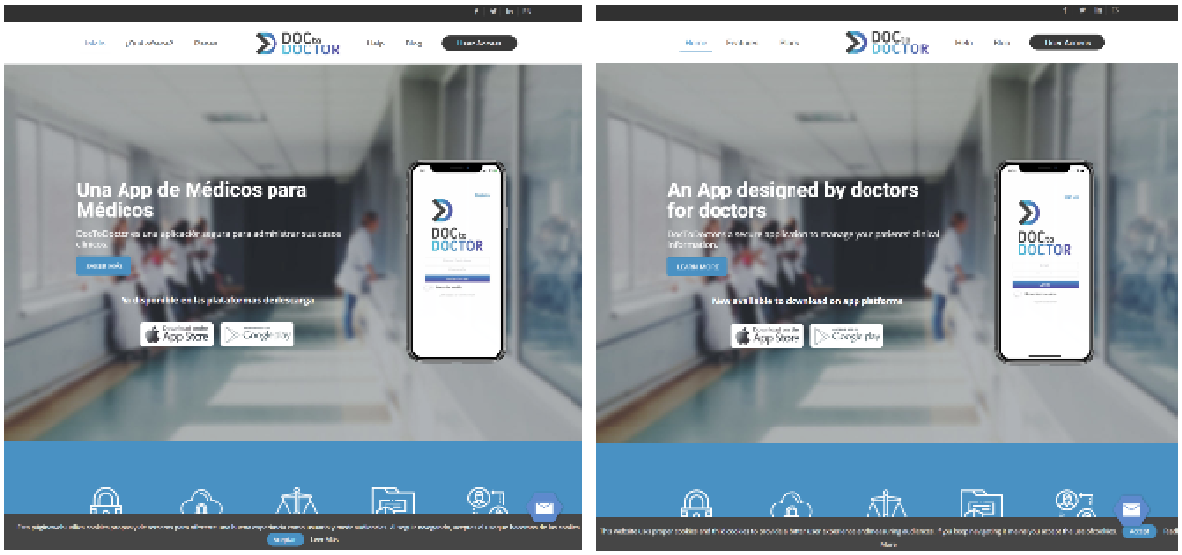
a) Confirmar el número de usuarios y volumen de datos afecto.
b) Informa a la Agencia Española de Protección de Datos
c) Informar a los usuarios mediante Notificación Push-in
d) Remitir correo electrónico narrando los pormenores del hecho

Si toda la información almacenada en los Servidores de Datos está correctamente anonimizada las posibilidades de triangular a un sujeto (y con ello identificarlo) en base a los datos acumulados es casi nula.

IV. PROYECCIÓN INTERNACIONAL

DocToDoctor©, primera iniciativa mundial de gestión de los datos de Salud que implementa el RGPD desde el diseño presenta un coremulti-idiomático desde el inicio. Actualmente es bilingüe Castellano e Inglés, con versiones en francés, alemán, italiano, ruso, y sueco en preparación.

La aplicación en sistemas iOS y Android, el soporte Web, la página web, y la documentación de Términos y Condiciones y Política de Privacidad se encuentran en Castellano e Inglés. Sucesivos lanzamientos en diversos países europeos irán acompañados de la traducción en el idioma nacional, al menos en los principales europeos.



Gráfica 12: Página Web doctodoctor.com en versión Español e Inglés (https://doctodoctor.com/)

DocToDoctor cumple por exceso los requisitos que preconiza la HealthInsurancePortability and AccountabilityAct federal norteamericana (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html), y la nueva reglamentación del Estado de California, que entra en vigor en 2020, denominada California ConsumerPrivacyActy que alberga expectativas dispares. Por ello, la aplicación ha despertado interés en USA y ya se cuenta con usuarios en ese país.

También existe una comunidad de usuarios en Argentina e Uruguay, pese a que su legislación nacional no ha alcanzado aún los estándares europeos, muchos profesionales conscientes de la Privacidad utilizan la aplicación por la protección que ofrece.

DocToDoctor© es un proyecto desarrollado en una comunidad ultraperiférica europea, las Islas Canarias, con vocación netamente internacional. Sin embargo, su compromiso ético que preconiza la Independencia frente a consorcios de acumuladores de datos o grandes farmacéuticas obliga a un crecimiento controlado y progresivo. V

V. CRITERIOS EMPRESARIALES

DocToDoctor© es una iniciativa personal de un médico comprometido con la Privacidad, el Dr. Armando Molina Betancor, colegiado en Santa Cruz de Tenerife, que ante la ausencia de soluciones a los conflictos éticos que la actividad profesional cotidiana presenta respecto a la inadecuación a las normas básicas de protección de privacidad, se propuso encontrar una respuesta que aunara el crecimiento del conocimiento personal del facultativo con el RGPD.

Tras establecer una Sociedad Limitada, Molinapps SLU, con capital propio, se ha contratado una empresa informática radicada en Canarias y con el know-how necesario para desarrollar el proyecto informático, Axedra/CanaryWeb.

La aplicación DocToDoctor© se encuentra disponible en los repositorios Apple Store y Google Play Store desde enero de 2019. No es una idea ni un proyecto, es una realidad efectiva y tangible.

DocToDoctor© es un proyecto ético independiente, que pretende proteger la información de Salud bajo los mismos criterios deontológicos que el propio ejercicio de la Medicina. Por ello, está comprometida desde su misma concepción es no ceder jamás datos de usuarios o de pacientes a terceros, y a no insertar publicidad o realizar spam.

DocToDoctor© pretende sostenerse mediante cuota abonada por los usuarios formando una comunidad ética, aunque ha previsto el desarrollo de planes de colaboración institucionales.

Precisamente por el compromiso ético, el destino manifiesto será la creación de una Fundación que tutele la protección de los datos de Salud incorporando a los diversos organismos públicos con implicaciones deontológicas (Colegios Profesionales, Servicios públicos de Salud…), cuando el crecimiento de la base de usuarios lo permita.

La comercialización de DocToDoctor©se lleva a cabo en 4 niveles de acceso dependiendo de la suscripción por el usuario.

1. Versión pre-verificación o Uso Protegido. Un Usuario No Verificado como Profesional Médico en ejercicio con Licencia válida podrá descargarse y manejar DocToDoctor© de forma local en su dispositivo con un límite de 10 episodios o documentos. No podrá enviar ni recibir ningún tipo de información mediante la app con ningún otro usuario o programa.

2. Versión gratuita o de Acceso. Un Usuario cuya identidad y actividad legal ha sido verificada, podrá guardar en su dispositivo hasta 25 episodios clínicos de sus pacientes incluyendo los Consentimientos (cifrados e inaccesibles), y podrá recibir episodios y fotos de otros usuarios con caducidad de 48 horas. Sin embargo, no tendrá soporte web de back-up y edición de fotos, ni podrá enviar fotos o datos a otros usuarios.

3. Versión individual. Este tipo de usuario por suscripción podrá almacenar en su dispositivo con soporte web un número ilimitado de episodios(existe limitación de espacio en Servidor), y podrá remitir información y episodios individualmente a otros usuarios (con caducidad de 48 horas para el receptor) con nivel de Acceso o superior. Contará con back-up en la nube cifrado y protegido, que podrá usar como almacenamiento permanente eliminando episodios del dispositivo para mantener la memoria ocupada en el dispositivo en límites razonables que no afecten al funcionamiento de otras aplicaciones. El precio oficial de la suscripción a este nivel es de 9.99 € por mes, con descuentos especiales por periodos más largos así como ofertas institucionales.

4. Versión de Grupos. Permite además de las capacidades anteriores, compartir el seguimiento de un paciente mediante el acceso y edición de múltiples usuarios a una copia del usuario original con un sistema propio que garantiza el cifrado individual del número de historial sin acceso a claves ajenas, valido para recoger la actividad en unidades clínicas, secciones, comisiones clínicas, grupos multidisciplinares, despachos compartidos, etc., en definitiva, en aquellos casos en que varios profesionales necesitan comunicarse para lograr una óptima atención clínica sobre un paciente. El costo de la suscripción es de 12.99€ por mes y usuario.

Suscripción	Características	Precio
Protegida	max. 10 elementos. No acceso	Gratuita
Acceso	max. 25 elementos. Puede *RECIBIR*	Gratuita
Individual	Ilimitados casos. Web*. ENVIAR* y recibir casos	9.99€/mes/user
Grupos	Ilimitados casos. Ilimitados grupos*MODIFICAR*	12.99€/mes/user

Tabla 08. Tipos de suscripción a DocToDoctor©

DocToDoctor©aspira a que se difunda por toda la clase médica de forma que esté presente en modo *Acceso*en la mayoría de los Facultativos nacionales y europeos, con el objetivo que se convierta en el *VISOR GRATUITO* por defecto de la información médica compartida con el cumplimiento del RGPD a efectos de segunda opinión o comentarios.

DocToDoctor© ofrece además herramientas para el usuario más sofisticado que precise mantener abiertas todas las opciones que se ofrecen en la web así como poder compartir sus casos, alcanzando además a aquellos grupos profesionales que cuidan conjuntamente la Salud de un paciente.

El desarrollo longitudinal de DocToDoctor©se encuentra en plena ejecución. Por confidencialidad empresarial no podemos mostrar la planificación de funciones pendientes, pero si podemos reseñar las fases cumplidas y las que están en pruebas, delineadas en la siguiente tabla:

F	Característica	Estado
1	Consentimiento y carrete protegido	Implementada
2	Compartir episodios individuales	Implementada
3	Compartir en grupo	Implementada
4	Notificaciones push-in y chat evanescente	Beta
5	…..	…
.	…..	…..
10	Gestor global de Información Médica	Planificado

Tabla 09. Desarrollo de Producto DocToDoctor©

Existe también el convencimiento de que la innovadora dinámica de datos que DocToDoctor©aporta, también tiene un *desarrollo transversal* a otros sectores que están sujetos también a Código Deontológico. El diseño y programación modular que se ha utilizado para los profesionales médicos se implementará en breve para otros colectivos de usuarios como los que constituyen Enfermería, Odontología, Fisioterapia, Matronas… y que puede extenderse a actividades que manejen datos protegidos aunque no sean de Salud, como Peritaciones, Inspecciones, Abogacía, etc.

Molinapps SL pretende alcanzar el pleno desarrollo sin acudir a las fuentes de financiación clásicas como Fondos de Inversión o Instituciones Bancarias, así como evita depender de Empresas Farmacéuticas o de Dispositivos Médicos, porque cree que la delicada naturaleza de los datos que maneja puede ser objeto de la codicia de las Corporaciones sustentadas en Datos (Data Barons), y el acceso a los mercados financieros se convierte en flanco débil para absorciones o pérdida del control de las aplicaciones comercializadas.

Molinapps SL se convierte así en una Start-Up que rehúsa el crecimiento explosivo sostenido en capital y aboga por el crecimiento orgánico sostenido por los Usuarios. Más lento, con menos impacto inmediato, pero la única forma ética de garantizar la integridad de los datos.

En un mundo donde se busca el beneficio máximo explotando cualquier resquicio susceptible de monetizarse, DocToDoctor© es un proyecto que busca sostenibilidad en la solidaridad profesional, asumiendo con ello criterios de desarrollo sostenible.

VI. PROTECCIÓN A COLECTIVOS DESFAVORECIDOS

Los pacientes y familiares expuestos a una enfermedad son per se miembros de un colectivo frágil y expuesto a situaciones de penosidad y sufrimiento. Pero dentro de ellos existen subgrupos que exigen además protección especial.

a. DocToDoctor© incorpora la protección a menores y pacientes **dependientes** desde su misma concepción. No sólo promueve conductas específicas de seguridad en su decálogo de normas para la Toma Ética de Fotos Médicas, sino que presenta mecanismos para recoger el Consentimiento de los Responsables Legales para el almacenamiento de datos de Salud de pacientes menores, inconscientes o dependientes, tan accesible y paralelo al de los pacientes con Autonomía legal y consciencia plena.

b. Un sistema seguro de recogida de imágenes tiene valor **Pericial**. DocToDoctor© protege de forma extrema la identidad de los pacientes. En situaciones en que se realizan exploraciones conjuntas entre Forenses y Facultativos Especialistas, habitual en Ginecología y Pediatría, DocToDoctor© dispone de un mecanismo para certificar la fecha y hora de la toma de imágenes, a la vez que oculta esa información al Servidor pues sólo es accesible en el dispositivo móvil protegido con código de seguridad. De esta forma, facilita la documentación y la “seguridad en la certeza” en casos de declaración en asuntos judiciales en situaciones de Violencia de Género y Abusos Sexuales.

VII. OBJETIVOS DE DESARROLLO SOSTENIBLE. Agenda 2030

La iniciativa DocToDoctor© se enmarca dentro de los siguientes ítems de los Objetivos de Desarrollo Sostenible de la Agenda 2030 de la Organización de Naciones Unidas:

Gráfica 13: Desarrollo Sostenible de la Agenda 2030 en que incide DocToDoctor©

(3) Salud y Bienestar.

DocToDoctor© es una herramienta para que los profesionales conscientes guarden los datos de pacientes que merecen estudio detenido posterior o seguimiento de resultados, para realizar un feed-back o retroalimentación de aprendizaje sobre casos que de otra forma se pierden en la vorágine de la presión asistencial. Esto redunda en que se potencia el desarrollo personal profesional, lo que beneficia al paciente en concreto, pues facilita al Médico que "se preocupa" de entrecruzar y recordar el resultado de pruebas o diagnósticos, y a los subsiguientes pacientes con patologías similares, al incrementar la pericia y conocimiento del profesional.

Además, DocToDoctor© permite compartir de forma segura el seguimiento de pacientes entre grupos de Facultativos mediante su función de Grupos, protegiendo igualmente la identidad del paciente, logrando alcanzar una Medicina Personalizada Multidisciplinar.

(4) Educación de Calidad.

DocToDoctor© se convierte en una herramienta básica de docencia imbricada en el RGPD, pues solicita el Consentimiento Específico del paciente para poder compartir sus datos e imágenes con colegas y en situaciones de enseñanza y publicaciones. La iconografía de las clases y ediciones se pude así hacer con imágenes autorizadas por los pacientes, y esta autorización se puede *demostrar* gracias a la aplicación.

(8) Trabajo Decente y Crecimiento Económico

El modelo ético solidario que ha elegido Molinapps SLU para la comercialización de DocToDoctor© es opuesto a la *maximización de beneficios en pro de los accionistas* que caracteriza la situación actual del mercado de fármacos, dispositivos sanitarios y, como no, la acumulación de datos. Tratar los datos de Salud con los mismos requerimientos éticos que conlleva el tratamiento de los pacientes y sus enfermedades debe llevarse a cabo con criterios de sostenibilidad del conjunto y no con acaparación de recursos económicos.

(12) Producción y Consumo Responsables + (15) Vida de Ecosistemas Terrestres.

DocToDoctor© tiene un considerable impacto en reducir la *huella en papel – huella de carbono*, pues la mayoría de Médicos que precisan registrar o recordar a algún paciente para seguimiento terminan imprimiendo una copia en papel de su historial clínico. Sucede, además y cotidianamente, con los Médicos Internos Residentes, que precisan recoger cada una de sus actuaciones para la realización de una Memoria Anual obligatoria [este asunto es la base de un Proyecto Docente Multicéntrico en preparación]. El ahorro de impresión en papel podría ser de miles de folios diariamente (en 2016 se calcularon en 28.114 médicos residentes en España, que recogen TODA su actividad diaria https://www.smandaluz.com/noticia/430/cuntos-facultativos-residentes-hay-en-espaa-en-marzo-de-2016).

Addenda1

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

RESPONSABLE DEL TRATAMIENTO

Molinapps SL

DESCRIPCIÓN DE LA ACTIVIDAD DE TRATAMIENTO

Actividad del tratamiento	Gestión de usuarios

Finalidad	Gestión de usuarios de la plataforma: comunicaciones electrónicas, validación, etc.
Interesados	Usuarios
Categorías de datos	Datos identificativos: • Nombre • Apellidos • DNI/NIF • Número de colegiado • Correo electrónico • Tratamiento

TRANSFERENCIAS INTERNACIONALES Y CESIONES

Cesiones	Empresa informática
Transferencias previstas	No se realizan transferencias internacionales
Periodo de conservación	5 años

CICLO DE VIDA DE LA ACTIVIDAD DE TRATAMIENTO

1. CAPTURA DE LOS DATOS

Actividades del proceso	Formulario de alta en la plataforma y formulario de modificación del perfil de usuario.
Datos tratados	Datos identificativos
Intervinientes	Usuarios / Empresa informática
Tecnologías	Sistemas informáticos

2. ALMACENAMIENTO DE LOS DATOS

Actividades del proceso	Se almacena la información en base de datos.
Datos tratados	Datos identificativos
Intervinientes	Usuarios / Empresa informática
Tecnologías	Sistemas informáticos

3. USO Y TRATAMIENTO DE LOS DATOS

Actividades del proceso	Gestión de usuarios: incidencias, comunicaciones electrónicas, información, etc.
Datos tratados	Datos identificativos
Intervinientes	Empleados / Empresa informática
Tecnologías	Sistemas informáticos

4. TRANSFERENCIAS Y CESIONES PREVISTAS

Actividades del proceso	• Gestión de incidencias • Mantenimiento de datos
Datos tratados	Datos identificativos
Intervinientes	Empleados / Empresa informática
Tecnologías	Sistemas informáticos

4. DESTRUCCIÓN

Actividades del proceso	Borrado seguro y definitivo de los sistemas informáticos
Datos tratados	Datos identificativos
Intervinientes	Empleados / Empresa informática
Tecnologías	Sistemas informáticos

MEDIDAS DE SEGURIDAD DEL RESPONSABLE DE TRATAMIENTO

Medidas de seguridad	• Seudonimización y cifrado de datos personales • Capacidad de garantizar la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento • Restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico. • Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas de seguridad técnicas adoptadas

ENCARGADO DEL TRATAMIENTO

1. DATOS DEL ENCARGADO DE TRATAMIENTO

Encargado del tratamiento	CanaryWeb, S. L. B38409892 Calle Fermín Morín, 2. Portal 1, local 6. 38007 Santa Cruz de Tenerife
Delegado de Protección de Datos	José Luis Luengo Barreto joselluengobarreto@gmail.com dataprotectionofficer@doctodoctor.com

2. DESCRIPCIÓN DE LOS TRATAMIENTOS DE DATOS

Responsable del tratamiento	CanaryWeb, S. L. B38409892 Calle Fermín Morín, 2. Portal 1, local 6. 38007 Santa Cruz de Tenerife
Categorías de tratamiento	Datos identificativos de usuarios

3. TRANSFERENCIAS Y CESIONES

Transferencias y cesiones previstas	No se hacen cesiones ni transferencias internacionales

4. MEDIDAS DE SEGURIDAD DEL ENCARGADO DEL TRATAMIENTO

Medidas de seguridad	• Seudonimización y cifrado de datos personales • Capacidad de garantizar la confidencialidad, integridad y disponibilidad de los sistemas y servicios de tratamiento • Restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico. Proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas de seguridad técnicas adoptadas

Addenda2

Pregunta realizada a la AEPD (justificante y texto)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

JUSTIFICANTE REGISTRO DE ENTRADA

Nº de Registro: 025086/2019
Fecha de Recepción: 19/05/2019 22:53:05

DATOS DE QUIEN PRESENTA LA SOLICITUD

Nombre: ARMANDO

Apellidos: MOLINA BETANCOR

Tipo Documento Identificativo: NIF

NIF/NIE/Pasaporte: 42802404W

Domicilio: MÉNDEZ NUÑEZ, NUM 56, PISO D, PTA. D

País: ESPAÑA

Provincia: SANTA CRUZ DE TENERIFE

Localidad: SANTA CRUZ DE TENERIFE

CódigoPostal: 38002

Teléfono: 609655457

Correo electrónico: MOLINAPPS@GMAIL.COM

MEDIO DE NOTIFICACIÓN

- ☐ Notificación Postal
- ☒ Notificación Electrónica

DATOS DEL INTERESADO

Razon Social: MOLINAPPS SL

Nif: B76712785

Domicilio: MENDEZ NUÑEZ, NUM 56, PISO 2, PTA. D

País: ESPAÑA

Provincia: SANTA CRUZ DE TENERIFE

Localidad: SANTA CRUZ DE TENERIFE

CódigoPostal: 38002

Teléfono: 609655457

Correo electrónico: MOLINAPPS@GMAIL.COM

MEDIO DE NOTIFICACIÓN

- ☐ Notificación Postal
- ☒ Notificación Electrónica

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

JUSTIFICANTE REGISTRO DE ENTRADA

Nº de Registro: 025086/2019
Fecha de Recepción: 19/05/2019 22:53:05

Detalles de la Solicitud de Registro

Tipo operación
REGISTRO INICIAL

Tipo documento
CONSULTA INFORMA RGPD

Unidad destino
SECRETARÍA GENERAL / REGISTRO E.S.

NºRegistro de Entrada	NºRegistro de Salida	NªExpediente

Consulta
PREGUNTA SOBRE FUNCIONALIDADES DE UNA APLICACIÓN DE TELEFONÍA MÓVIL PARA MÉDICOS

Documentos Adjuntos

Nombre	Descripción	Hash del documento	Tamaño
Molinapps__Consulta_AEPD_DocToDoctor_texto.DOCX	TEXTO DE LA PREGUNTA	6zA/aaAZ62cM/Ry3KlVcreSONDk=	2316968 bytes
D2D_1.jpg	PRIMERA PÁGINA FIRMADA	DtNP6Terg2sA382ov8M9j5Nuwz4=	806247 bytes
D2D_8.jpg	ÚLTIMA PÁGINA FIRMADA	l78f+NO6K4PfTDfgYvRKLdbYO88=	585233 bytes

CLÁUSULA INFORMATIVA

Los datos de carácter personal serán tratados por la Agencia Española de Protección de datos e incorporados a la actividad de tratamiento "Registro de E/S", cuya finalidad es la gestión del registro de entrada y salida de documentos de la Agencia Española de Protección de Datos, en los términos previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

JUSTIFICANTE REGISTRO DE ENTRADA

Nº de Registro: 025086/2019
Fecha de Recepción: 19/05/2019 22:53:05

Finalidad basada en el cumplimiento de una obligación por la Agencia Española de Protección de Datos.

Los datos de carácter personal serán comunicados a los órganos administrativos a los que, en su caso, se dirija la documentación, de acuerdo con lo previsto en el artículo 16 de la Ley 39/2015.

Los datos se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se han recabado y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. Será de aplicación la normativa de archivos y patrimonio documental español.

Puede ejercitar sus derechos de acceso, rectificación, supresión y portabilidad de sus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos, cuando procedan, ante la Agencia Española de Protección de Datos, C/Jorge Juan, 6, 28001- Madrid o en la dirección de correo electrónico dpd@agpd.es

A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

D. José Luis Luengo Barreto, en nombre y representación de **Molinapps, S.L.** ("**Molinapps**"), con dirección en Calle Méndez Núñez número 56, 38002, Santa Cruz de Tenerife (España), actuando en su calidad de Delegado de Protección de Datos ante la Agencia Española de Protección de Datos ("**AEPD**") comparezco y, como mejor proceda en Derecho,

DIGO

I. Que Molinapps es la entidad titular de la aplicación móvil DocToDoctor (en adelante, la "**App**"), disponible tanto para sistemas operativos *Android* como *IOS*, cuya finalidad es ofrecer a los profesionales sanitarios (en concreto, a médicos colegiados con licencia activa verificada —y no a la generalidad de los usuarios—) un sistema de almacenamiento y compartición, privada y cifrada, de información médica. Puede obtenerse mayor información sobre está App en https://doctodoctor.com/es/inicio/.

II. Para garantizar la seguridad de la información, DocToDoctor guarda la información disociada en dos servidores diferentes:

(a) un **Servidor de Identidades** que contiene los datos de los usuarios (nombre, apellidos, país, número de colegiación profesional, datos de facturación, etc.) así como los consentimientos firmados por los pacientes (cifrados y sin acceso automático). Todos los datos y documentos aquí almacenados se cifran utilizando OpenSSL y el algoritmo AES-256-CBC. Este servidor sólo es accesible desde el Servidor de Datos de forma unidireccional. Esto quiere decir que se pueden dar de alta nuevas identidades, pero no se pueden hacer consultas de forma automática. La conexión desde el Servidor de Datos está protegida mediante certificado SSL.

(b) un **Servidor de Datos** que mantiene seudonimizado al paciente, mediante el cifrado del número de historial (sea de centro, consulta, clínica, etc., sin geolocalización), y también mantiene cifradas las fotos, notas y comentarios de cada caso. El cifrado se lleva a cabo utilizando OpenSSL y el algoritmo AES-256-CBC. Todas las conexiones desde los dispositivos móviles y al Servidor de Identidades están protegidas mediante certificado SSL.

III. Que, debido a razones médicamente necesarias y legítimas para que los médicos intercambien la información sanitaria de sus pacientes con otros compañeros de profesión, Molinapps está considerando la comercialización de una nueva funcionalidad que permita a los médicos registrados en la App compartir la información que suministren sobre sus pacientes con otros médicos registrados con fines de diagnóstico y/o investigación, en el marco de sus tareas profesionales (el "**Servicio Compartir**").

IV. Que, dada la importancia y el carácter de la información y la incidencia adicional que supone en el ámbito de la protección de datos personales, Molinapps desea saber si, en cumplimiento de sus obligaciones como encargado del tratamiento, las medidas de seguridad técnicas y organizativas que ha diseñado e implementado son apropiadas al riesgo derivado del Servicio Compartir.

V. Que, a tal fin, Molinapps presenta respetuosamente ante la AEPD la siguiente

CONSULTA
A LA AEPD ACERCA DEL SERVICIO COMPARTIR DE MOLINAPPS

1. **SUPUESTO DE HECHO**

1.1 **Introducción a la App**

1.1.1 Como ya se ha definido, la App consiste en una herramienta de trabajo hecha por médicos para médicos, ideada con el objeto primordial de proteger la confidencialidad, privacidad e intimidad de los pacientes y de los médicos, así como la seguridad de los mismos.

1.1.2 La App nació con el objetivo de evitar la práctica extendida entre los profesionales sanitarios de conservar la documentación confidencial y privada de sus pacientes en sus hogares o dispositivos personales, así como su comunicación a terceros a través de aplicaciones de mensajería instantánea gratuitas, que facilita el acceso incidental a la información confidencial de sus pacientes por parte de familiares, conocidos o terceros, de forma del todo insegura, o en última instancia la pérdida de dicha información; exponiendo a los pacientes a un altísimo e injustificado riesgo de vulneración de sus derechos a la privacidad y la protección de datos. Todo ello, a su vez, sin perjuicio de los deberes de los profesionales de cuidado, confidencialidad y secreto. Sobre todo teniendo en cuenta la sensibilidad de cualesquier dato relativo a los pacientes.

1.1.3 Así, la App ofrece a los profesionales sanitarios o médicos un método para guardar y almacenar de forma cifrada, segura y confidencial determinada información sobre sus pacientes (los "**Pacientes**"), de la que son responsables, en sus dispositivos móviles, incluyendo soporte de back-up y acceso seguro en la nube (el "**Servicio de Almacenamiento**").

Para ello es necesario crear un código personal de, como mínimo, 4 dígitos para acceder a las funcionalidades de la App. Este código es necesario reintroducirlo si el usuario salta a otra aplicación o la deja inactiva por más de 5 minutos. Además, el código permite acceder a funciones avanzadas y a los datos cifrados en el dispositivo. Este dato no se almacena nunca en nuestros servidores.

La App ofrece herramientas para recortar (no pixelar) la información de filiación de un paciente o centro que pudiera haberse agregado a una foto o documento.

Asimismo, la App ofrece otras medidas de seguridad como la posibilidad de difuminar las imágenes mientras se navega por los datos y fotos de paciente (Blur Mode), protegiendo tanto la seguridad de la información como la sensibilidad del observador inadvertido, dada la en ocasiones crudeza de las imágenes profesionales médicas.

Además, se incluyen servicios accesorios o adicionales relativos a la organización de la información.

1.1.4 Dado que la App se dirige a médicos colegiados y con licencia activa (los "**Profesionales**" o "**Usuarios**" de la App), se solicita como requisito para el registro en la App el número de colegiación así como el envío de prueba a este respecto:

Es decir, no está "abierta" a todos los usuarios, lo cual refuerza su carácter profesional y su naturaleza como herramienta de trabajo, así como limita su uso a profesionales sometidos a deberes deontológicos y de confidencialidad reforzados.

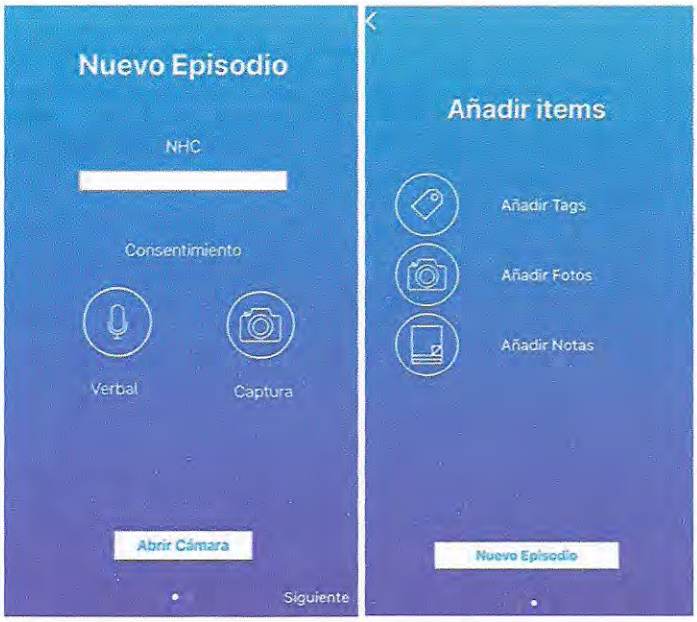
1.1.5 Con respecto a los datos de los Pacientes (los "**Datos de Pacientes**"), el Profesional es el responsable de su tratamiento y recogida, así como del cumplimiento de todas las obligaciones regulatorias y de protección de datos frente a los Pacientes. Es el Profesional quien decide qué datos recoger del Paciente, qué datos almacenar en la App y, en última instancia, qué datos se retiran de la App. Estos Datos de Pacientes podrán constar de imágenes, resultados clínicos u otros datos (entre otros, su imagen/voz o categorías especiales de datos incluyendo datos relativos a la salud como la historia clínica). El Profesional es quien decide si cargar o no en la App estos Datos de Pacientes, como responsable del tratamiento de los mismos.

1.1.6 En conclusión, Molinapps se considera a sí misma una prestadora de servicios de la sociedad de la información de "*cloud computing*" o computación en la nube y, bajo la normativa aplicable de protección de datos, encargada del tratamiento de los datos facilitados por los Profesionales sobre sus Pacientes, bajo su dirección e instrucción.

1.2 **El Servicio Compartir**

1.2.1 Como se ha anunciado anteriormente, junto con el Servicio de Almacenamiento, Molinapps está analizando implementar el Servicio Compartir, consistente en permitir no solo el almacenamiento de los Datos de Pacientes en la App, sino también la compartición de los mismos con otros Usuarios (i.e. Profesionales) de la App con fines de diagnóstico y/o investigación, bien directamente de Usuario a Usuario, o mediante la creación de grupos de Usuarios. Explicamos el funcionamiento de dicho servicio a continuación.

1.2.2 Cuando un Profesional debidamente registrado decide crear un nuevo "*Episodio*" (es decir, un registro, ficha o caso relativo a un Paciente nuevo o sobre el que ya se haya subido otro Episodio) en la aplicación, se indexa el número de historia clínica ("**NHC**"), que corresponde al número de historial de un centro sanitario, consulta privada o asistencia de pacientes. Este es el único dato que es indexado.



1.2.3 Este NHC se cifra originalmente en el dispositivo móvil en el momento de introducirlo. El Servidor de Identidades lo recibe cifrado y para almacenarlo en el Servidor de Datos lo cifra de nuevo utilizando OpenSSL y el algoritmo AES-256-CBC. De esta manera la cadena de texto cifrada original no se ve comprometida ante un posible ataque al Servidor de Datos. El NHC en claro (descifrado) es solo accesible en el dispositivo móvil introduciendo la clave de usuario correcta, ya que el Servidor de Datos nunca almacena la clave de usuario. La clave personal, al ser un código numérico presenta ciertas limitaciones, pero se ve fortalecido cuando aplicamos una derivación de clave utilizando el estándar PKCS#5. Este estándar basa su derivación de claves en técnicas de "Salting", para añadir aleatoriedad a la clave; y "Key Stretching", para añadir dificultad computacional a la propia derivación de la clave. Esto hace que la clave que se genera para el cifrado sea fuerte frente a ataques de "de diccionario" (es decir, probando distintas palabras de forma automática) o "fuerza bruta" (es decir, probando todas las posibles combinaciones hasta dar con la contraseña oportuna).

1.2.4 Además, cada episodio se registra en el Servidor de Datos de Molinapps con un seudónimo que consiste en:

> Las iniciales del Profesional + ordinal de esas iniciales + contador del número de casos que ese profesional vaya introduciendo en el sistema.

Por ejemplo, si el Profesional se llamase Ana Garcia y solo ha subido un caso a la App: AG170001.

1.2.5 Todos los datos del Paciente, o documentos que permitan identificarlo, se disocian (como ya se ha explicado) completamente del resto de datos clínicos del paciente apoyándonos en el Servidor de Identidades. En el momento en el que se crea un paciente nuevo, el Servidor de Datos envía los datos de ese paciente y solicita al Servidor de Identidades la creación de una nueva identidad. Una vez creada, el Servidor de Identidades proporciona un identificador único que es utilizado por el Servidor de Datos para agrupar los datos clínicos que almacena. Los datos del paciente enviados no se almacenan en ningún momento en el Servidor de Datos y tampoco podrán ser consultados posteriormente.

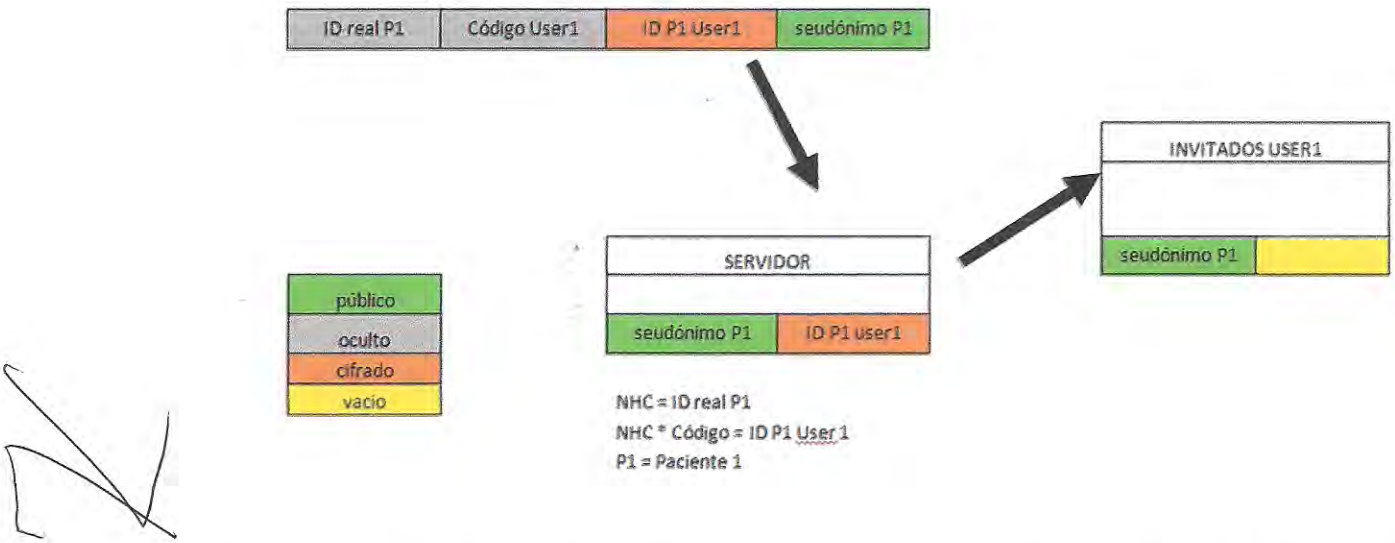
1.2.6 En conclusión, el Servidor de Datos únicamente contendrá el seudónimo creado por la App referente a los Datos de Pacientes y el NHC cifrado.

1.2.7 Un Usuario podrá compartir la información de un Paciente, una imagen o un caso completo (imágenes, anotaciones, descripciones y etiquetas) con otro Usuario registrado en la App, pero en dicha información:

(a) Solo se comparte el seudónimo (**nunca** el número de historial original) y además el acceso a esta información es **temporal**, eliminándose del dispositivo receptor a las 48 horas; y

(b) Cada fotografía contiene, aparte de metadatos cifrados, una marca de agua (logotipo traslúcido con códigos insertados) y diversos elementos de esteganografía (en distintas fases de implantación) —que actualmente se encuentran en fase de desarrollo— con el objetivo de que exista **trazabilidad** del flujo de información, y conocer quién, cuándo y a quién se remitió determinada imagen.

En el dispositivo del Usuario, se aplica su clave o código personal (*"Código User1*" en la imagen a continuación) al NHC (*"ID real P1*" en la imagen a continuación) para obtener un ID cifrado por Paciente y Usuario (*"ID P1 User 1*" en la imagen a continuación). Dicho ID permite al Usuario poner en relación la información con el seudónimo (que es el dato indexado que se comparte). De esta forma, en el Servidor de Datos de Molinapps solo se almacena el seudónimo y el ID del Paciente cifrado.



1.2.8 Asimismo, el Servicio Compartir permite que varios Usuarios puedan crear **grupos de trabajo** en que pueden compartir y modificar la información. En este punto nos encontramos con la problemática del cifrado del NHC del paciente, ya que como comentamos previamente, éste sólo es descifrable en el dispositivo del propietario del caso y con la clave correspondiente.

Para solucionar esto, hemos implementado un algoritmo que permite almacenar el NHC del Paciente de forma tan segura como en los casos individuales. El algoritmo funciona de la siguiente manera:

1. Un Usuario crea un grupo y, a su vez, crea una clave de grupo numérica para este grupo de forma similar a la clave de acceso personal (*"Código Grupo*" en la imagen a continuación).

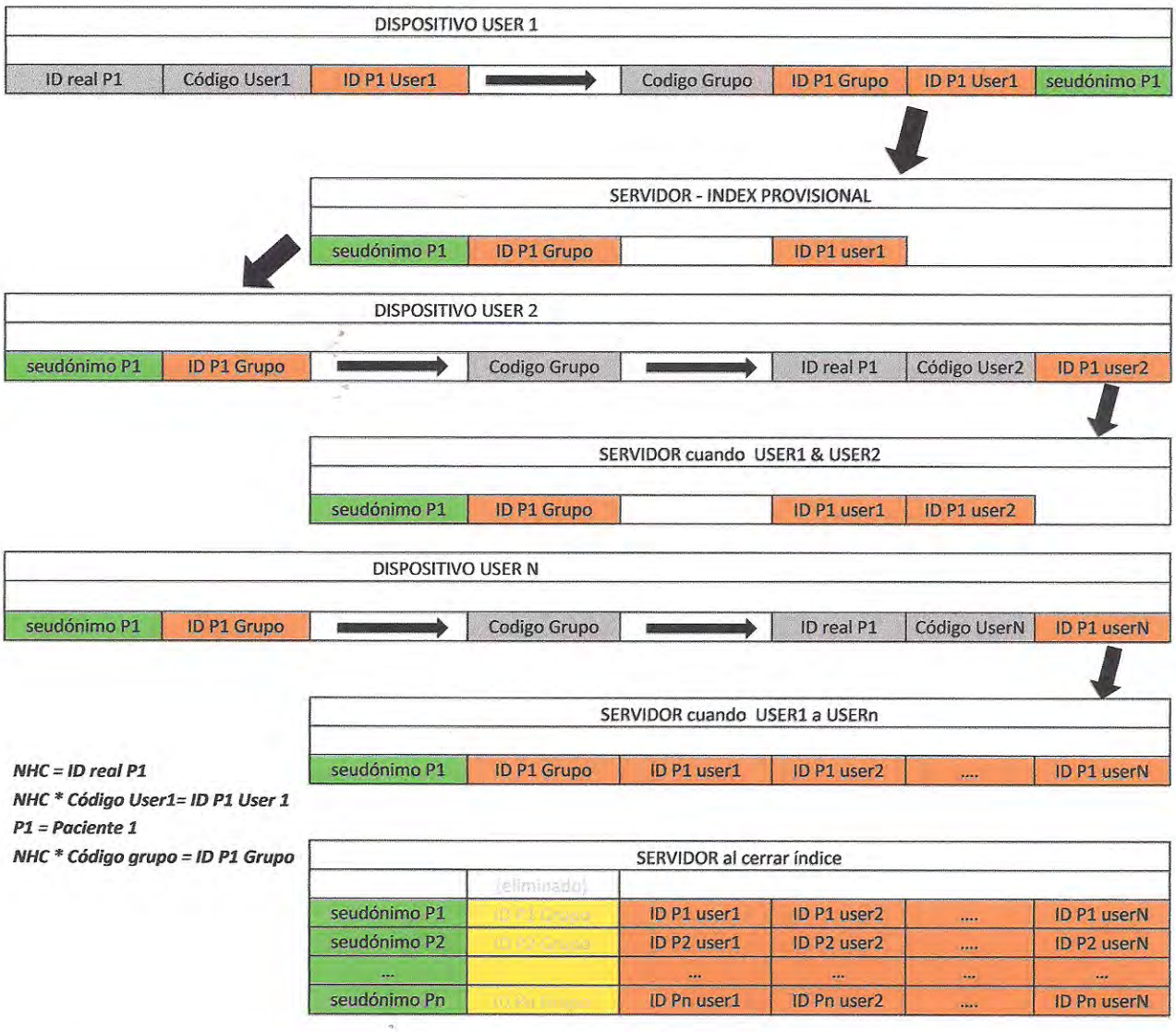
2. Al añadir un caso o episodio al grupo, se cifra el NHC del paciente con la clave de grupo generando lo que llamamos ID de Grupo (*"ID P1 Grupo*" en la imagen a continuación). Este ID de grupo es temporal hasta que los miembros del grupo sincronicen sus dispositivos.

3. Los usuarios que reciban la invitación al grupo recibirán igualmente la clave de grupo que deberán introducir en el dispositivo para descifrar los IDs de grupo de los casos o episodios compartidos.

4. En el momento de la sincronización inicial de un caso o episodio, el Usuario lo recibirá con el ID de grupo, por lo que será necesario descifrarlo con la clave de grupo y se volverá a cifrar con la clave personal, generando un nuevo ID de Usuario para ese paciente (*"ID P1 User X*" en la imagen a continuación). Este nuevo ID se sincroniza con el Servidor de Datos y se elimina el antiguo ID de grupo del paciente y miembro del grupo correspondiente (ver "*SERVIDOR al cerrar índice*" en la imagen a continuación).

5. En el servidor cada caso tendrá tantos identificadores como usuarios integren el grupo. Cada uno de ellos cifrado con la clave personal de cada miembro e inaccesible para el resto.

Con este algoritmo resolvemos la problemática existente y el NHC sigue estando cifrado y almacenado de forma segura sin que el servidor tenga conocimiento del NHC real en ningún momento.



2. LAS PROBLEMÁTICA PLANTEADA Y OPINIÓN DE MOLINAPPS

2.1.1 Dada la sensibilidad de la información contenida en la App, esto es, los Datos de Pacientes; y el aumento de la incidencia en la esfera de la protección de datos que la nueva funcionalidad supondría respecto de los Datos de Pacientes; Molinapps como encargada del tratamiento y proveedora de servicios vela por ofrecer a sus clientes (i.e. los Profesionales debidamente acreditados) y, en última instancia, a los Pacientes de estos, el mayor grado de seguridad y confidencialidad posible.

Por este motivo, Molinapps ha optado por implementar de forma proactiva para los Profesionales una herramienta de trabajo funcional y en fiel cumplimiento a los principios de privacidad desde el diseño y por defecto previstos en el artículo 25 del Reglamento General de Protección de Datos (Reglamento [UE] 2016/679 o "**RGPD**").

2.1.2 En este punto, en Molinapps se ha apostado por implementar reforzadas medidas de seguridad, incluyendo un sistema de cifrado por capas que minimice los riesgos de re-identificación de los Pacientes, a la vez que mantenga su utilidad para los Profesionales (y así evitar que terminen en otras aplicaciones que, gracias a su funcionalidad y difusión en el mercado, aseguran una mayor masa crítica de clientes sin necesidad de implementar las medidas de seguridad más apropiadas).

En concreto, el RGPD recoge en su artículo 32 referido a la *Seguridad del Tratamiento* que los encargados del tratamiento (así como los responsables) deberán implementar medidas de seguridad apropiadas para garantizar un nivel de seguridad adecuado al riesgo, especificando concretamente, entre otros la "*seudonimización y el cifrado de datos personales*".

2.1.3 De esta forma, el sistema implementado en la App y el funcionamiento para el Servicio Compartir se ha diseñado sobre los siguientes cimientos protectores de los datos facilitados por los Profesionales, es decir, por los responsables del tratamiento de dichos datos que deciden depositar los mismos, así como su confianza, en Molinapps:

(a) El primer dato básico que el Profesional facilita del Paciente es el NHC, número que depende de cada hospital, centro sanitario, consulta privada o asistencia de pacientes. Es decir, la App opera sobre la base de un dato que en sí mismo es poco identificador al no señalar el nombre del Paciente, del hospital o la enfermedad del sujeto y, en última instancia, que genera poco riesgo de identificación del individuo.

(b) Se lleva a cabo un cifrado del NHC y se genera un seudónimo como se ha explicado en el punto 1.2.3. anterior. Este seudónimo es el dato que comparte, junto con el ID del Usuario.

(c) La información compartida se borra del dispositivo receptor de la misma a las 48 horas.

(d) Con respecto a las imágenes que se suban a la App, se habilita a los Usuarios una opción que permite recortar la imagen (no simplemente pixelar), para evitar la identificación de los Pacientes afectados.

(e) Con respecto a la creación de los grupos, en el apartado 1.2.8. se desarrolla el sistema de creación de ID de grupos y de Usuarios que, a su vez, se elimina del Servidor de Datos de Molinapps para incrementar la seguridad.

(f) No se debe olvidar que DocToDoctor es una App cuyo objeto es su uso como herramienta de trabajo por parte de Profesionales debidamente colegiados. Es decir, su uso se desarrolla en el ámbito de profesionales médicos sometidos a estrictos deberes de secreto, confidencialidad médico-paciente, y deberes deontológicos. En ningún caso se permite su acceso a terceros ni al público en general.

Es decir, el ámbito subjetivo sobre el que se desarrolla la App es limitado y especialmente reservado. De nuevo, siguiendo con la idea constitutiva de asegurar la privacidad desde el diseño y por defecto.

En todo caso, no hay que olvidar que, bajo Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("**LOPD**"), se prohíbe que estos Profesionales receptores de Datos de Pacientes (así como cualquier tercero) lleven a cabo "[l]*a reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados*", la cual se califica como una infracción muy grave.

(g) Por último, se obliga contractualmente a los Usuarios, vía los Términos y Condiciones (https://doctodoctor.com/es/terminos-y-condiciones/) que tienen que aceptar para hacer uso de la App, a primar la privacidad, protección de datos y confidencialidad de los Datos de Pacientes. En particular, se recomienda que, en la medida de lo posible, eviten la inclusión de datos personales relativos a Pacientes.

2.1.4 Con todos estos mecanismos implementados, Molinapps desea confirmar con la AEPD que las medidas de seguridad implementadas en la App se consideran medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo y que tienen 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. Es decir, que Molinapps, en su condición de encargado del tratamiento, cumple adecuadamente con su obligación de tomar todas las medidas de seguridad necesarias de conformidad con el artículo 32 RGPD y el artículo 28.3.c) RGPD.

3. CONSULTAS A LA AEPD

A la vista de lo expuesto, Molinapps plantea respetuosamente la siguiente consulta a la Agencia Española de Protección de Datos:

¿Se puede considerar que el sistema integral de seguridad implementado por Molinapps es apropiado al riesgo derivado del Servicio Compartir, en relación con sus obligaciones bajo los artículos 32 y 28.3.c) RGPD?

Por las razones expuestas, a la Agencia Española de Protección Datos, Molinapps respetuosamente,

SOLICITA

- Que de por presentada esta consulta y, previo los trámites oportunos, tenga a bien responderla.
- Que esa Agencia dirija cualquier comunicación que desee realizar a Molinapps en relación con esta consulta, a la siguiente persona y dirección:

D. Gonzalo F. Gállego Higueras

Hogan Lovells International

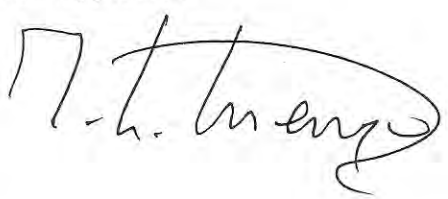
Paseo de la Castellana, 51 - 28046 Madrid, España

Tel: +34 91 3498200 Fax: +34 913498201

Correo electrónico: gonzalo.gallego@hoganlovells.com

En Santa Cruz de Tenerife, a 20 de mayo de 2019

Molinapps, S.L.



D. José Luis Luengo Barreto

Addenda 3

Publicaciones en prensa

EL PAÍS

https://elpais.com/tecnologia/2019/01/24/actualidad/1548353697_774503.html

Publicado: 26/01/2019

Canarias7
Toda la información de Canarias

https://www.canarias7.es/sociedad/sanidad/un-medico-canario-crea-una-app-que-protege-los-datos-del-paciente-ED7115475

Publicado: 28/04/2019

Diario de Avisos

https://diariodeavisos.elespanol.com/2019/02/armando-molina-creador-de-doctodoctor-esta-aplicacion-unica-en-el-mundo-da-respuesta-a-lo-que-necesitamos-los-medicos/

Publicado: 12/02/2019

AMENAZA ROBOTO

https://amenazaroboto.com/doc-to-doctor

Publicado: 18/03/2019

LA VANGUARDIA

https://www.lavanguardia.com/vida/20190214/46463481625/una-aplicacion-convierte-el-movil-en-un-canal-seguro-para-los-datos-medicos.html

Publicado: 04/02/2019

https://www.diariodealcala.es/2019/01/28/la-caja-fuerte-digital-de-la-informacion-medica/

Publicado: 11/03/2019

Revista Acta Medica (Del Colegio Oficial de Médicos de Santa Cruz de Tenerife)

https://medicostenerife.es/wp-content/uploads/2019/05/ActaM%C3%A9dica_234_A3_WEB.pdf

Publicado: Nº 234 - Julio 2019