risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido / Recibido: 09/04/2014
Aceitação / Aceptación: 01/06/2014

Seguridad y Privacidad en Carpetas Personales de Salud para Android e iOS

Belén Cruz Zapata [1], Antonio Hernández Niñirola [1], José Luis Fernández-Alemán [1], Ambrosio Toval [1]

b.cruzzapata@um.es, antonio.hernandez5@um.es, aleman@um.es, atoval@um.es

1 Grupo de Investigación de Ingeniería del Software, Departamento de Informática y Sistemas, Facultad de Informática, Universidad de Murcia – Campus de Espinardo, 30100, Murcia, España.

DOI: 10.4304/risti.13.35-50

Resumen: Durante los últimos años, el uso de dispositivos móviles como teléfonos inteligentes y tabletas ha suscitado gran interés entre los proveedores de servicios de salud en el mundo de la mSalud. Las Carpetas Personales de Salud (en inglés Personal Health Record o PHR) móviles proporcionan numerosas ventajas y aunque hay estudios que indican que los pacientes están dispuestos a utilizarlos, los índices de uso son aún bajos. La seguridad y la privacidad han sido identificadas como una importante barrera para lograr su amplia adopción. Haciendo uso de un método adaptado de la revisión sistemática de literatura se identificaron 24 PHRs móviles para Android e iOS. La seguridad y privacidad de estos PHRs móviles fueron evaluadas usando un cuestionario de 12 preguntas. Nuestra investigación muestra que los desarrolladores de PHRs móviles han de mejorar sustancialmente sus políticas de privacidad.

Palabras-clave: mSalud; Carpeta Personal de Salud Móvil; Android; iOS.

Privacy and Security in Mobile Personal Health Records for Android and iOS

Abstract: In the last few years, the increment in use of mobile devices such as smartphones and tablets has caused the interest of health service providers in the world of mHealth. Mobile Personal Health Records (mPHR) lead to a number of benefits and there are studies that notice how patients are willing to use them. However, utilization rates are low. Security and privacy have been identified as important adoption barriers and should therefore be addressed. Using a method similar to the well-known Systematic Literature Review, 24 mPHRs for Android and iOS were identified. The security and privacy of the mPHRs were evaluated through a questionnaire containing 12 questions. Our research shows that mPHRs developers should improve significantly their privacy policies.

Keywords*:* mHealth; Mobile Personal Health Records; Android; iOS.

1. Introducción

El uso de Internet para acceder información médica es un fenómeno relativamente reciente y se conoce como eSalud (Oh, Rizo, Enkin, & Jadad, 2005). Los pacientes son más conscientes y tienen un rol más activo en la gestión de su información médica (Van De Belt, Engelen, Berben, & Schoonhoven, 2010). Tanto es así, que un cinco por ciento de las búsquedas registradas en Google están relacionadas con el mundo de la salud (Eysenbach & Köhler, 2004). Existen estudios que afirman que los pacientes están dispuestos a utilizar Carpetas Personal de Salud (en inglés Personal Health Records o PHRs) y que los profesionales de la medicina valoran y recomiendan el uso de estos programas (Huba & Zhang, 2012) (Fernández Alemán, Hernández, & Sánchez García, 2013). Los PHRs son aplicaciones que permiten a un individuo acceder, modificar y compartir su información médica (Kaelber & Pan, 2008) (Carrion, Fernandez Aleman, & Toval, 2012).

Los PHRs están disponibles en distintos formatos: USB, aplicaciones para PC, aplicaciones web, entre otros (World Health Organization, 2011). Con la gran evolución del mercado de aplicaciones móviles, las aplicaciones médicas en general (mSalud) y los PHRs en particular, han llegado al mundo móvil (World Health Organization, 2011). El informe del Mercado de Salud Móvil (Mobile Health Market Report) de 2013-2017 calcula que habrá más de 500 millones de usuarios de aplicaciones de mSalud en 2015 (Jahns & Houck, 2013). Los PHRs móviles (mPHRs) permiten a los pacientes acceder a su información médica en cualquier momento y en cualquier lugar (Kharrazi, Chisholm, VanNasdale, & Thompson, 2012).

A pesar de la buena predisposición de los consumidores hacia los mPHRs, existe aún una baja tasa de utilización (Fernández Alemán et al., 2013)(Archer, Fevrier-Thomas, Lokker, McKibbon, & Straus, 2011). Se han identificado en la literatura numerosas barreras en la adopción de los PHRs: usabilidad, conflictos culturales, problemas legales y preocupación por la privacidad y seguridad (Liu, Shih, & Hayes, 2011; Lober et al., 2006; Tang, Ash, Bates, Overhage, & Sands, 2006). Un estudio norteamericano de 2003 realizado a 1.246 consumidores, indica que la preocupación por mantener la privacidad y seguridad de la información personal de salud aparece en un 91% de los encuestados (Markle Foundation, 2003). Un 25% de los participantes indicaron incluso que dejarían de utilizar el PHR si existieran problemas con la privacidad. Aun así, la mayoría de encuestados creen que la tecnología proporciona medidas de seguridad apropiadas para mantener su información clínica segura. El objetivo de nuestro trabajo es analizar las características de seguridad y privacidad que tienen los actuales mPHRs. Para alcanzar este objetivo, se ha realizado un análisis de las políticas de privacidad de 24 mPHRs.

El artículo se organiza de la siguiente forma: en la Sección 2 se describe la metodología empleada en el proceso de evaluación de las políticas de privacidad de los mPHRs. En la Seccion 3 se exponen los resultados obtenidos y se describen las características principales de las políticas de privacidad evaluadas. En la Sección 4 se discuten los hallazgos principales del estudio. Por último, en la Sección 5 se sintetizan las conclusiones y se describen trabajos futuros.

2. Metodología

La búsqueda de mPHRs se realizó mediante la adaptación para aplicaciones móviles del proceso de revisión sistemática de la literatura aplicado en Ingeniería del Software (Brereton, Kitchenham, Budgen, Turner, & Khalil, 2007). Una revisión sistemática de la literatura permite identificar, evaluar, interpretar y sintetizar todos los aspectos relevantes de un tema de interés concreto (Pino, García, & Piattini, 2006). El proceso utiliza métodos formales para asegurar la efectividad y la imparcialidad de los resultados obtenidos. También se siguieron las directrices presentadas en el informe PRISMA (Preferred Reporting Items for Systematic reviews and Meta-Analysis) (Moher, Liberati, Tetzlaff, & Altman, 2009). El método fue desarrollado previamente al inicio de las tareas de búsqueda e incluye los criterios de elegibilidad, las fuentes de información y describe los procesos de selección de aplicaciones y de extracción y recolección de datos.

2.1. Criterios de Elegibilidad

En esta sección se presentan los Criterios de Inclusión (CI) y los Criterios de Exclusión (EC). Para que una aplicación sea seleccionada, ésta ha de cumplir todos y cada uno de los Criterios de Inclusión.

- CI1: mPHRs de carácter general: no centradas en alguna condición de salud concreta como por ejemplo diabetes o embarazo.
- CI2: mPHRs que están disponibles de manera gratuita.
- CI3: mPHRs que han sido actualizados posteriormente al 1 de enero de 2013.

Las aplicaciones que cumplieron con al menos uno de los siguientes Criterios de Exclusión fueron descartadas.

- CE1: mPHRs que al ser evaluados presentan errores de instalación o de tiempo de ejecución que no permiten la correcta evaluación de la aplicación.
- CE2: mPHRs que dependen completamente de un servicio externo (de pago o gratuito) y no pueden ser evaluadas independientemente como aplicaciones móviles sino como conjunto de servicios.

2.2. Fuentes y Cadena de Búsqueda

Nuestra investigación se centró en aplicaciones para las dos plataformas móviles más extendidas actualmente: Android e iOS. Las aplicaciones disponibles para iOS se encuentran centralizadas en el repositorio de Apple oficial App Store. Para Android existen otros repositorios además de Google Play, repositorio oficial de aplicaciones de Google para Android, como Amazon Appstore. Se optó por elegir como fuentes de información los repositorios oficiales: Google Play para Android y App Store para iOS. Estos dos repositorios son líderes mundiales tanto en número de aplicaciones disponibles como en número de descargas. Si nos centramos en aplicaciones bajo la categoría de Salud, ambos repositorios tienen un gran repertorio de aplicaciones: existen alrededor de 20.000 aplicaciones médicas en la App Store y más de 8.000 en Google Play (Aungst, 2013).

Ambos repositorios tienen disponibles motores de búsqueda que fueron empleados para el proceso de búsqueda de las aplicaciones. La cadena de búsqueda se elaboró haciendo uso de los criterios PICO (Stone, 2002): "PHR" O "Personal Health Record".

2.3. Selección de los mPHRs

El proceso de selección de mPHRs se llevó a cabo siguiendo las siguientes fases:

1) El uso de la cadena de búsqueda previamente definida en los motores de búsqueda de los repositorios App Store de Apple y Google Play de Google.
2) La exploración manual de la información disponible en la descripción de los mPHRs en los repositorios para aplicar los Criterios de Inclusión.
3) La exploración manual de la información disponible en la descripción de los mPHRs en los repositorios y de los mPHRs en sí para aplicar los Criterios de Exclusión.
4) La exploración manual de los mPHRs, de la información disponible en la descripción de los mPHRs en los repositorios y en algunos casos de las páginas web de las aplicaciones o de los desarrolladores para identificar las políticas de privacidad de cada mPHR.
5) Lectura completa de cada política de privacidad, extracción y recolección manual de las características de seguridad evaluadas.

2.4. Proceso de Extracción y Recolección de la Información

Cada mPHR fue evaluado de manera independiente por dos de los autores del estudio. Las discrepancias fueron resueltas mediante discusión entre los mismos dos autores. El proceso de extracción y recolección de la información fue realizado haciendo uso de formularios de extracción de datos presentados en forma de hojas de cálculo.

2.5. Evaluación de calidad

La evaluación de los mPHRs se llevó a cabo a través del uso de un cuestionario de doce cuestiones definidas por los autores disponible en la Tabla 1. La estructuración del cuestionario está basada en los Principios de Buenas Prácticas de la Información (Fair Information Practice Principles, FIPPs) de la Comisión General de Comercio de EEUU (Federal Trade Comission, FTC). Estos principios son internacionalmente aceptados y ampliamente usados en la creación de políticas de privacidad, estando además centrados en la recolección de datos de los usuarios (Wu, Huang, Yen, & Popova, 2012). Se establecen cinco principios: notificación, elección, acceso, seguridad y ejecución. Notificación, es el principio fundamental por el que el usuario debe ser informado de las prácticas que va a realizar la empresa con su información personal antes de que ésta sea registrada; Elección, el usuario debe conocer las opciones sobre cómo va a ser usada su información, si la información va a ser revelada a una tercera entidad y bajo qué condiciones; Acceso, el usuario debe poder acceder a sus datos para modificarlos o eliminarlos; Seguridad, los datos del usuario y su integridad debe ser protegida; Ejecución, consiste en las acciones legales a seguir si la política de privacidad es violada. El último principio sobre ejecución queda fuera del ámbito de nuestro análisis.

Cada respuesta está asociada con una puntuación: S (Sí) = 2, P (Parcialmente) = 1, - (No Procede) = 0, N (No) = 0. El proceso de evaluación fue realizado

independientemente por dos de los autores haciendo uso de hojas de cálculo. Las diferencias fueron discutidas hasta alcanzar un acuerdo entre los propios autores. Para medir el nivel de acuerdo se ha usado el índice Kappa de Cohen (Landis & Koch, 1977), el cual es una medida estadística para evaluar la concordancia entre observadores de variables cualitativas. El índice obtenido es de 0.9717 lo cual indica un grado de concordancia muy alto.

Tabla 1. Cuestionario de evaluación de las políticas de privacidad

Notificación	
C1	*¿Es la política de privacidad fácilmente accesible?*
	S (Sí), la política de privacidad está disponible desde el propio mPHR; P (Parcialmente), la política de privacidad está disponible en la descripción del mPHR en el repositorio, en la página web del mPHR o en la página web del desarrollador; N (No), la política de privacidad no está disponible.
C2	*¿Son los cambios en la política de privacidad notificados al usuario?*
	S (Sí), los cambios en la política de privacidad son notificados cuando el usuario utiliza el mPHR por primera vez después de que se hayan producido los cambios; P (Parcialmente), los cambios se notifican mediante una actualización en la propia política de privacidad, incluyendo la fecha del cambio; N (No), los cambios en la política de privacidad se producen sin notificación alguna.
C3	*¿Se informa al usuario del uso de Cookies, servicios de análisis de datos, servicios de geo-localización o almacenamiento de IPs?*
	S (Sí), se informa al usuario del uso de Cookies, servicios de análisis de datos, servicios de geo-localización o almacenamiento de IPs; N (No), no se hace uso de Cookies, servicios de análisis de datos, servicios de geo-localización ni almacenamiento de IPs.
C4	*¿Sigue el mPHR algún estándar o recomendación de seguridad?*
	S (Sí), el mPHR cumple con algún estándar o recomendación de seguridad; N (No), el mPHR no cumple con ningún estándar.
Elección	
C5	*¿Existe algún mecanismo de acceso a los datos en caso de emergencia médica?*
	S (Sí), existe un mecanismo de acceso a los datos del paciente en caso de emergencia; N (No), no existe mecanismo de acceso a los datos del paciente en caso de emergencia.
C6	*Si el mPHR permite conexión con otros PHRs o EHRs, ¿se explicita las condiciones de dicha conexión?*
	S (Sí), el mPHR permite la conexión con otros PHRs o EHRs y se explicita cómo se realiza y asegura la comunicación; N (No), el mPHR permite la conexión con otros PHRs o EHRs pero no se explicita cómo se realiza y asegura la comunicación; - (No Procede), el mPHR no permite la conexión con otros PHRs ni con EHRs.

Acceso	
C7	*Si el mPHR permite múltiples usuarios, ¿se puede conceder y revocar acceso a otros usuarios? ¿Qué tipos de accesos permite?*
	S (Sí), el mPHR permite múltiples usuarios y permite conceder y revocar acceso a datos de otros usuarios de sólo lectura y de lectura-escritura; P (Parcialmente), el mPHR permite múltiples usuarios y permite conceder y revocar acceso a datos de otros usuarios pero no permite especificar qué tipo de acceso; N (No), el mPHR permite múltiples usuarios pero no permite conceder y revocar acceso a datos de otros usuarios; - (No Procede), el mPHR no permite múltiples usuarios.
Seguridad	
C8	*¿Utiliza el mPHR un mecanismo de autenticación fuerte?*
	S (Sí), el proceso de autenticación está basado en dos o más de los siguientes elementos: 1) algo que el usuario conoce (ej. usuario y contraseña), 2) algo que el usuario posee (ej. tarjeta de autenticación) y 3) algo que el usuario es (ej. biometría); P (Parcialmente), el proceso de autenticación está basado en solamente uno de los elementos citados anteriormente; N (No), no existe proceso de autenticación.
C9	*Si se almacenan datos localmente, ¿están encriptados? ¿Qué mecanismo de encriptación se utiliza?*
	S (Sí), existen datos almacenados localmente y se explicita cómo están encriptados; P (Parcialmente), existen datos almacenados localmente y los datos están encriptados, pero no se explicita cómo están encriptados; N (No), existen datos almacenados localmente pero no son encriptados; - (No procede), no existen datos almacenados localmente.
C10	*Si se transfieren datos online, ¿están encriptados? ¿Qué mecanismo de encriptación se utiliza? ¿Qué protocolo de comunicación segura utiliza?*
	S (Sí), existen transferencias de datos y se explicita cómo son encriptados y cuál es el protocolo de comunicación; P (Parcialmente), existen transferencias de datos y los datos son encriptados, pero no se explicita cómo o cuál es el protocolo de comunicación; N (No), existen transferencias de datos pero no son encriptados; - (No Procede), no se transmiten datos.
C11	*Si se almacenan datos en la nube, ¿están encriptados? ¿Qué mecanismo de encriptación se utiliza? ¿Se explicita si hay control de acceso, auditoría y la protección física de los servidores?*
	S (Sí), existen datos almacenados en la nube y se explicita cómo están encriptados y las medidas de seguridad que se toman para garantizar la integridad y seguridad de los servidores; P (Parcialmente), existen datos almacenados en la nube y los datos están encriptados, pero no se explicita cómo están encriptados ni las medidas de seguridad que se toman para garantizar la integridad y seguridad de los servidores; N (No), existen datos almacenados en la nube pero no están encriptados; - (No Procede), no existen datos almacenados en la nube.
C12	*Si el mPHR permite la creación de copias de seguridad, ¿cómo se garantiza la seguridad sobre dicha copia?*
	S (Sí), el mPHR permite la creación de copias de seguridad y éstas son protegidas; N (No), el mPHR permite la creación de copias de seguridad pero no se protegen; - (No Procede), el mPHR no permite la creación de copias de seguridad.

3. Resultados

En esta sección se presentan los resultados obtenidos. La primera sección presenta los resultados obtenidos en el proceso de búsqueda y selección de los mPHRs. En la segunda sección están disponibles las características más relevantes de las políticas de seguridad extraídas a través la evaluación de los mPHRs seleccionados.

3.1. Selección de los mPHRs

La búsqueda de los repositorios de aplicaciones seleccionados generó un total de 203 aplicaciones posibles. Un total de 139 aplicaciones fueron descartadas por no cumplir el CI1, trece fueron descartadas por no cumplir el CI2 y dieciséis por no cumplir el CI3. Finalmente se aplicaron los Criterios de Exclusión: 6 mPHRs fueron excluidos por cumplir el EC1 y otros 5 por cumplir el EC2. Al final, 24 mPHRs fueron seleccionados y sus características de privacidad y seguridad fueron evaluadas. El proceso completo resumido puede ser consultado en el diagrama de flujo PRISMA en la Figura 1.

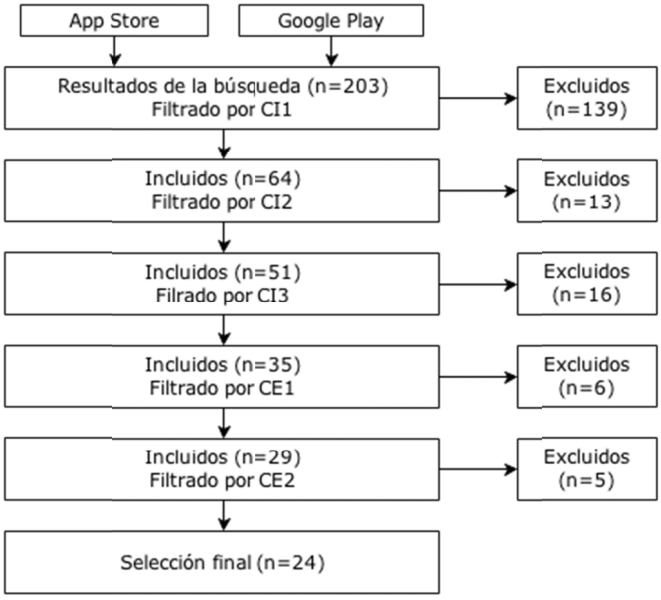

Figura 1. Diagrama de flujo PRISMA

3.2. Características de los mPHRs

Para identificar las características más relevantes de las políticas de seguridad analizadas se aplicó el cuestionario de 12 preguntas previamente desarrollado a las políticas de privacidad de los mPHRs seleccionados. Los resultados para cada cuestión del cuestionario así como la puntuación total obtenida pueden ser consultados en la Tabla 2.

Notificación

La primera característica a evaluar fue si la política de privacidad está disponible de manera rápida y sencilla para los usuarios del mPHR. Tres de los 24 mPHRs evaluados (*CareFlow PHR*, *MyWelness App* y *Personal Health Record – Lite*) no tienen política de privacidad. En el caso de la aplicación *CareFlowPHR,* se indica una URL para consultar la política, pero este sitio web no existe. De forma similar, la aplicación *MyWellnessApp* informa que la política de privacidad se encuentra en su página web oficial, pero en ésta realmente no puede ser encontrada. Otros dos mPHRs (*EasyMed*

Medical Passport para Android e iOS) no tienen la política de privacidad disponible directamente desde la aplicación y hay que visitar la página web del desarrollador.

Tabla 2. Evaluación de las políticas de privacidad de los mPHRs seleccionados

mPHR	OS	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	T
CareFlowPHR	And	N	-	-	-	-	-	N	P	-	-	-	-	1
CareSync	iOS	S	P	S	N	N	-	P	P	P	P	P	-	10
EasyMed Medical Passport	iOS	P	N	S	N	N	-	N	P	-	N	S	-	6
EasyMed Medical Passport	And	P	N	S	N	N	-	N	P	-	N	S	-	6
Health Companion	iOS	S	P	S	N	N	-	N	P	-	P	N	-	7
Health suite	And	S	N	S	N	N	-	-	N	N	-	-	-	4
Health2me	iOS	S	P	S	N	N	-	N	P	-	N	N	-	6
Health2me	And	S	P	S	N	N	-	N	P	-	N	N	-	6
HealthStylus	iOS	S	N	N	N	N	-	N	P	N	P	P	-	5
HealthStylus	And	S	N	N	N	N	-	N	P	N	P	P	-	5
iBlueButton	iOS	S	P	S	N	N	-	-	P	P	P	-	-	8
iTriage Health	And	S	P	S	S	N	S	N	P	-	N	P	-	11
iTriage Health	iOS	S	P	S	S	N	S	N	P	-	N	P	-	11
LifeCard Health Record	iOS	S	S	S	N	N	-	N	P	N	N	P	-	8
MTBC PHR	And	S	P	S	N	S	-	N	P	P	S	S	-	13
MTBC PHR	iOS	S	P	S	N	S	-	N	P	P	S	S	-	13
My Health Diary	And	S	P	S	N	N	-	N	P	-	P	P	-	8
MyClinicNotes	iOS	S	P	S	N	N	-	N	P	-	S	P	-	9
MyMx Personal Health Record	iOS	S	P	N	N	N	-	-	N	P	P	S	-	7
MyWellnessApp	iOS	N	-	-	-	-	-	-	N	-	-	-	-	0
OnPatient Medical Record PHR	And	S	P	N	S	N	-	N	P	-	N	P	-	7
OnPatient Personal Health Record	iOS	S	P	N	S	N	-	N	P	-	N	P	-	7
Personal Health Record – Lite	iOS	N	-	-	-	-	-	-	N	-	-	-	-	0
Track My Medical Records	And	P	N	N	N	N	-	N	P	-	S	P	-	5
Total		**39**	**16**	**30**	**8**	**4**	**4**	**1**	**20**	**5**	**15**	**21**	**0**	**163**

Los cambios en la política de privacidad son notificados al usuario a través de la aplicación en sólo un caso: *LifeCard Health Record*. El 65% de los mPHRs informan al usuario de los cambios mediante una actualización de la fecha del último cambio de la política.

El uso de cookies, servicios de análisis de datos, servicios de geo-localización y de almacenamiento son notificados en la política de privacidad en quince de los mPHRs evaluados: 13 de ellos realizan análisis de datos sobre el tipo de dispositivo y el uso del servicio, 8 mPHRs avisan sobre la utilización de cookies, 7 registran la dirección IP y 2 obtienen la localización del dispositivo. Estos dos últimos mPHRs, *iTriage Health* para Android y para iOS, justifican la extracción de la localización para ofrecer servicios y contenidos adaptados a ésta. Respecto a los estándares y recomendaciones, únicamente cuatro (16,66%) cumplen con el acta americana HIPAA (Health Insurance Portability and Accountability Act).

Elección

El acceso a datos en caso de emergencia se permite únicamente en *MTBC PHR* para Android e iOS. En dicha política de privacidad se indica explícitamente el acceso a los datos a familiares o amigos autorizados en casos de un riesgo inminente a la salud del paciente, o a especialistas médicos capaces de solventar o mitigar posibles problemas en casos de salud pública.

La comunicación con otros servicios similares de carpetas personales de salud sólo se produce en dos mPHRs del mismo desarrollador: *iTriage Health* para iOS y Android. Esta aplicación permite la sincronización de ciertos datos con *Microsoft HealthVault* ("Microsoft HealthVault," n.d.) o con *MyActiveHealth* ("MyActiveHealth," n.d.). En ambos casos se explicita en la política de privacidad que la comunicación se realiza de forma segura.

Acceso

El 79,16% (19 de 24) de los mPHRs analizados permiten múltiples usuarios, pero excepto uno, no es posible la conexión entre ellos ni el acceso a datos ajenos. *CareSync* es el único mPHR que permite otorgar y revocar el acceso a datos de otros usuarios. Sin embargo, no se puede especificar qué tipo de acceso (sólo lectura, sólo escritura, lectura/escritura, etc.).

Seguridad

El método de autenticación más extendido es el tradicional formado por usuario y contraseña (19 de 24 mPHRs). Sólo *Health Companion* emplea un sistema diferente basado en un código PIN de 4 cifras. *Health Suite*, *MyMx PHR*, *MyWelnessApp* y *Personal Health Record – Lite* no tienen ningún método de autenticación propio.

Sólo 9 aplicaciones almacenan datos localmente en el dispositivo móvil, el resto requieren de conexión a internet y transfieren los datos desde el servidor cada vez que el usuario quiere consultarlos. En cinco de las nueve políticas de privacidad de los mPHRs que almacenan datos localmente se especifica que los datos se guardan de forma segura. Las otras cuatro no dicen nada al respecto.

MyClinicNotes, Track My Medical Records y MTBC PHR para iOS y Android son las únicas aplicaciones que garantizan la seguridad en las transferencias de datos entre cliente y servidor e indican cómo se protege dicha conexión. En estos mPHRs, el método de protección de la comunicación empleado es SSL. Además, MTBC PHR indica que los datos se protegen con un método de encriptación de 128-bits de VeriSign. Otros cinco mPHRs indican que la comunicación entre cliente y servidor es segura pero no se especifica el método por el cual está protegido.

En cuanto a la información almacenada en la nube, cinco (20,83%) mPHRs no hacen uso de este servicio por lo que dependen de las copias de seguridad manuales del usuario para salvaguardar los datos. En los casos en los que sí se utiliza un servicio de almacenamiento online, cinco mPHRs indican que la integridad y seguridad de los servidores está garantizada mediante los mecanismos necesarios aportados por una empresa especialista externa. En otros 11 casos, simplemente se indica que la información está protegida pero no se especifica cómo.

Ninguno de los mPHRs estudiados permite realizar copias de seguridad. Técnicamente, aquellos mPHRs que almacenan datos localmente pueden hacer de una copia de seguridad de la información que contiene el dispositivo, mediante métodos como sincronización con iTunes o iCloud en el caso de iOS, o a través de alguna de las múltiples aplicaciones de copias de seguridad en Android.

4. Discusión

En esta sección se resumen y discuten las características de las políticas de privacidad de los mPHRs.

Notificación

Casi todos los mPHRs estudiados ofrecen un fácil acceso a su política de privacidad, estando ésta en la propia aplicación móvil. El usuario debería siempre poder acceder a la política de privacidad (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002). La opción más común es mostrar la política de privacidad en el momento en que el usuario realiza el proceso de registro, de forma que debe ser aceptada para poder completar el registro. Además, dada la importancia de la política de privacidad, los cambios realizados sobre ésta deben ser notificados al usuario (Carrión Señor, Fernández-Alemán, & Toval, 2012).

En las tecnologías web y móviles, es posible registrar información complementaria que no es proporcionada directamente por el usuario: tipo de dispositivo, sistema operativo, navegador web, dirección IP, tiempo permanecido en una página, historial de navegación en la aplicación, etc. Investigaciones realizadas entre 1998 y 2003 reflejan que el 62% de los usuarios se muestran preocupados por el hecho de que su actividad en Internet sea monitorizada (Kobsa, 2007). La utilización de cookies, además de aumentar la preocupación de los usuarios, puede suponer una vulnerabilidad de seguridad. Cuando las cookies son creadas para recordar los datos de acceso del usuario, un atacante podría interceptar esta información y acceder a la cuenta del usuario. Es importante por ello asegurar que las cookies de sesión sean

difícilmente predecibles, establecer límites de tiempo, no crear cookies persistentes o utilizar SSL para su envío (Palmer, 2007).

Elección

Las carpetas personales de salud cuentan con un problema inherente que es el acceso a los datos en casos de emergencia, es decir, cuando el usuario no puede acceder u otorgar acceso a otros usuarios. Pueden aparecer dos escenarios (van der Linden, Kalra, Hasman, & Talmon, 2009): consentimiento explícito, que significa que el usuario consiente las reglas de acceso establecidas en el caso de emergencia a menos que indique lo contrario; consentimiento implícito, que significa que el usuario prohíbe el acceso a menos que él lo conceda.

Añadir accesos en caso de emergencia añade un nivel extra de complejidad al proceso de autenticación e incrementa el riesgo de la integridad de los datos (van der Linden et al., 2009). Por otro lado, existen estudios que afirman que no todos los usuarios son propensos a compartir su información médica en casos de emergencia. Los pacientes con una salud buena o excelente están menos dispuestos a compartir sus datos en caso de una situación de este tipo (Weitzman, Kaci, & Mandl, 2010).

Acceso

De los mPHRs evaluados, solo uno contaba con un sistema para otorgar y revocar permisos de acceso a otros usuarios. Este sistema es bastante básico ya que no cuenta con funcionalidades más elaboradas presentes en otros PHRs para web o escritorio (Carrión Señor et al., 2012): distintos permisos sobre los datos (sólo lectura, lectura/escritura, modificación, etc.), permisos para acceder ciertos datos en concreto, registros de quién y cuándo ha accedido qué información, etc. Para cumplir las recomendaciones internacionales, tanto HIPAA como ISO 13606, es imprescindible que se notifique a los usuarios cómo se ha compartido su información médica (International Organization for Standardization, 2011; US Department of Health and Human Services, Office for Civil Rights, 2008).

Seguridad

Los mecanismos de autenticación son necesarios para evitar accesos no autorizados a la información del usuario. Ninguno de los mPHRs hace uso de un mecanismo de autenticación fuerte. Más del 80% de los mPHRs estudiados usa un mecanismo de autenticación compuesto únicamente de algo que el usuario conoce: la combinación de su nombre de usuario y contraseña. La información relativa a la salud requiere mecanismos de autenticación más seguros (Al-Nayadi & Abawajy, 2007). Si bien es cierto que los usuarios se muestran preocupados sobre la seguridad y privacidad, también buscan mecanismos de autenticación más sencillos, como es el caso de técnicas biométricas (Rodrigues & Santos, 2013). Los métodos de autenticación biométricos analizan las huellas dactilares, la voz o la retina del usuario (Zuniga, Win, & Susilo, 2010).

Catorce (58.33%) de los mPHRs son parte de un PHR perteneciente al ámbito web, pudiendo el usuario acceder a su información tanto desde el sitio web, como desde la aplicación móvil. La información de salud del usuario se almacena en servidores externos y no en el propio dispositivo móvil. El almacenamiento local de los datos se

puede producir de forma temporal si en ese momento, el dispositivo carece de conexión a la red. Cuando la información procede de varias fuentes, surgen más riesgos para la seguridad y privacidad de la información (Carrión Señor et al., 2012), pues se amplía el número de puntos de ataque y su variedad. Además, cuando la información de un PHR es almacenada en la nube, los usuarios pierden el control físico de sus datos y aumenta su desconfianza. Aunque muchos desarrolladores de mPHRs delegan en una empresa externa especializada en ofrecer este tipo de servicios, como *HOST* o *Amazon Web Services*, se debe cumplir la legislación sobre protección de datos vigente en cada país (Fernández-Alemán, Señor, Lozoya, & Toval, 2013). Es indispensable asegurar la confidencialidad, integridad y disponibilidad de la información de salud (Li, Yu, Ren, & Lou, 2010). Entre los mPHRs que indican qué método utilizan para garantizar la seguridad en las transferencias de datos entre cliente y servidor, el protocolo criptográfico SSL es el más extendido utilizándose en cuatro de cinco casos. SSL evita ataques del tipo intermediario (del término inglés Man-in-the-Middle), por el cual un atacante podría acceder a la información del usuario cuando ésta es transferida. Cuando la información se almacena localmente, y es el propio usuario quien gestiona las copias de seguridad, los mecanismos de sincronización y de copia de seguridad no siempre cifran los datos, y aunque lo hagan como es el caso de iCloud de iOS, pueden aparecer vulnerabilidades (Cliff Saran, 2014). Por tanto, medidas adicionales por parte de los desarrolladores de las aplicaciones son recomendables para garantizar la seguridad de los datos en las copias de seguridad.

4.1. Comparativa entre mPHRs y PHRs web

En un artículo reciente, se evaluaron las políticas de privacidad de 24 herramientas PHRs para web gratuitas (Carrión Señor et al., 2012). Si comparamos los resultados obtenidos en el presente estudio sobre mPHRs con los obtenidos para PHRs web, podemos afirmar que las políticas de privacidad en los mPHRs son menos rigurosas y más incompletas que en los PHRs web. En un 63% de los PHRs web analizados, se tuvieron en cuenta las regulaciones, recomendaciones o principios de seguridad, frente al 16% encontrado en los mPHRs. Además, el 71% de los PHRs web permite conceder y revocar permisos de acceso mientras que sólo un 4% de los mPHRs ofrece esta funcionalidad. Si nos centramos en aspectos de seguridad, obtenemos evidencia en el mismo sentido: los PHRs web son más seguros que los mPHRs. Un 63% de los PHRs web indica las medidas de seguridad físicas que utiliza, frente a un 20% en los mPHRs. Además, un 67% de los PHRs web indica las medidas de seguridad durante la transferencia de datos en línea, mientras que entre los mPHRs esto sólo sucede en un 16% de los casos.

5. Conclusiones

Las políticas de privacidad de los mPHRs son en general menos rigurosas y completas que las equivalentes para web o escritorio. La funcionalidad de las aplicaciones en materia de privacidad y seguridad también se encuentra menos desarrollada. Aunque las políticas de privacidad suelen estar disponibles de forma rápida y sencilla para el usuario, los cambios en estas políticas no suelen ser notificados y es el usuario el que debe estar atento ante posibles actualizaciones. En materia de elección, los usuarios están más restringidos al ser aplicaciones relativamente simples que no permiten en

general compartir información con familiares o profesionales de la salud. La integración con otros sistemas de información de salud externos como otros PHRs o EHRs también es escasa. La estructura y el contenido de las políticas de privacidad deben ser renovados para incluir información más detallada sobre medidas de seguridad cuando los datos se almacenan localmente, son transferidos por la red o se almacenan en servidores remotos.

Las características identificadas en este artículo y el cuestionario de 12 preguntas desarrollado pueden ser utilizadas por usuarios de mPHRs, profesionales de la salud y desarrolladores de aplicaciones móviles para evaluar sus aplicaciones en cuestión de privacidad y seguridad.

Referencias bibliográficas

Al-Nayadi, F., & Abawajy, J. H. (2007). An Authentication Framework for e-Health Systems. In *2007 IEEE International Symposium on Signal Processing and Information Technology* (pp. 616–620).

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. A., & Straus, S. E. (2011). Personal health records: a scoping review. *Journal of the American Medical Informatics Association*, *18*(4), 515–522.

Aungst, T. (2013, July 12). Apple app store still leads Android in total number of medical apps. *iMedicalApps*. Retrieved October 17, 2013, from http://www.imedicalapps.com/2013/07/apple-android-medical-app/

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software*, *80*(4), 571–583.

Carrion, I., Fernandez Aleman, J., & Toval, A. (2012). Personal Health Records: New Means to Safely Handle our Health Data? *Computer*, *45*(11), 77–33.

Carrión Señor, I., Fernández-Alemán, J. L., & Toval, A. (2012). Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies. *Journal of Medical Internet Research*, *14*(4), e114.

Cliff Saran. (2014, February 24). Apple users at risk of SSL man-in-the-middle attacks. Retrieved July 4, 2014, from http://www.computerweekly.com/news/2240214897/Apple-users-at-risk-of-SSL-man-in-the-middle-attack

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, § Official Journal of the European Communities (2002). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:en:PDF

Eysenbach, G., & Köhler, C. (2004). Health-related searches on the Internet. *JAMA: The Journal of the American Medical Association*, *291*(24), 2946. doi:10.1001/jama.291.24.2946

Fernández Alemán, J. L., Hernández, I., & Sánchez García, A. B. (2013). Opinion survey on the use of personal health records in the Region of Murcia (Spain). *Gaceta sanitaria / S.E.S.P.A.S*, *27*(5), 454–458.

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: a systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562.

Huba, N., & Zhang, Y. (2012). Designing patient-centered personal health records (PHRs): health care professionals' perspective on patient-generated data. *Journal of Medical Systems*, *36*(6), 3893–3905.

International Organization for Standardization. (2011). *ISO/TS 13606-4:2009: Health informatics -- Electronic Health Record Communication -- Part 4: Security*. Retrieved from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50121

Jahns, R.-G., & Houck, P. (2013). Mobile Health Market Report 2013-2017. Retrieved November 23, 2013, from http://www.research2guidance.com/shop/index.php/mobile-health-trends-and-figures-2013-2017

Kaelber, D., & Pan, E. C. (2008). The Value of Personal Health Record (PHR) Systems. *AMIA Annual Symposium Proceedings*, *2008*, 343–347.

Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: An evaluation of features and functionality. *International Journal of Medical Informatics*, *81*(9), 579–593.

Kobsa, A. (2007). The Adaptive Web. In P. Brusilovsky, A. Kobsa, & W. Nejdl (Eds.), (pp. 628–670). Berlin, Heidelberg: Springer-Verlag.

Landis, J. R., & Koch, G. G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*(1), 159–174.

Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings. In S. Jajodia & J. Zhou (Eds.), *Security and Privacy in Communication Networks* (pp. 89–106). Springer Berlin Heidelberg.

Liu, L. S., Shih, P. C., & Hayes, G. R. (2011). Barriers to the Adoption and Use of Personal Health Record Systems. In *Proceedings of the 2011 iConference* (pp. 363–370). New York, NY, USA: ACM.

Lober, W., Zierler, B., Herbaugh, A., Shinstrom, S., Stolyar, A., Kim, E., & Kim, Y. (2006). Barriers to the use of a Personal Health Record by an Elderly Population. *Proceedings of the AMIA Annual Symposium*, *2006*, 514–518.

Markle Foundation. (2003). *Connecting For Health: The Personal Health Working Group Final Report*. New York, NY. Retrieved from http://www.policyarchive.org/handle/10207/bitstreams/15473.pdf

Microsoft HealthVault. (n.d.). *Microsoft HealthVault*. Retrieved April 3, 2014, from http://www.healthvault.com

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Annals of Internal Medicine*, *151*(4), 264–269.

MyActiveHealth. (n.d.). *MyActiveHealth*. Retrieved April 3, 2014, from http://www.myactivehealth.com

Oh, H., Rizo, C., Enkin, M., & Jadad, A. (2005). What is eHealth (3): a systematic review of published definitions. *Journal of Medical Internet Research*, *7*(1), e1.

Palmer, S. (2007). *Web Application Vulnerabilities: Detect, Exploit, Prevent*. Syngress Publishing.

Pino, F. J., García, F., & Piattini, M. (2006). Revisión Sistemática de Mejora de Procesos Software en Micro, Pequeñas y Medianas Empresas. *Revista Española de Innovación, Calidad E Ingeniería Del Software*, *2*(001), 6–23.

Rodrigues, P., & Santos, H. (2013). Health users' perception of biometric authentication technologies. In *Proceedings of the IEEE 26th International Symposium on Computer-Based Medical Systems* (pp. 320–325).

Stone, P. (2002). Popping the (PICO) question in research and evidence-based practice. *Applied Nursing Research*, *15*(3), 197–8.

Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association*, *13*(2), 121–126.

US Department of Health and Human Services, Office for Civil Rights. (2008). *Personal Health Records and the HIPAA Privacy Rule*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf

Van De Belt, T. H., Engelen, L. J., Berben, S. A., & Schoonhoven, L. (2010). Definition of Health 2.0 and Medicine 2.0: A Systematic Review. *Journal of Medical Internet Research*, *12*(2).

Van der Linden, H., Kalra, D., Hasman, A., & Talmon, J. (2009). Inter-organizational future proof EHR systems: A review of the security and privacy related issues. *International Journal of Medical Informatics*, *78*(3), 141–160.

Weitzman, E. R., Kaci, L., & Mandl, K. D. (2010). Sharing Medical Data for Health Research: The Early Personal Health Record Experience. *Journal of Medical Internet Research*, *12*(2), e14.

World Health Organization. (2011). *mHealth: New horizons for health through mobile technologies*. Retrieved from http://www.who.int/goe/publications/ehealth_series_vol3/en/

Wu, K.-W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, *28*(3), 889–897.

Zuniga, A. E. F., Win, K. T., & Susilo, W. (2010). Biometrics for Electronic Health Records. *Journal of Medical Systems*, *34*(5), 975–983.