INFORMACIÓN PARA LOS INVESTIGADORES SOBRE PROTECCIÓN DE DATOS EN APLICACIONES PARA MÓVILES O TABLETAS (APPS).

DOCUMENTACIÓN QUE DEBEN REMITIR AL CEIC/CEIm

Las aplicaciones móviles pueden tratar datos personales que permiten incidir en la vida privada de los usuarios y terceras personas y que en ocasiones pueden referirse a información personal especialmente sensible y protegida.

Las Autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29), han publicado su Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, en el que recuerdan que el marco legal aplicable a cualquier *app* dirigida a los usuarios europeos es la Directiva de Protección de Datos 95/46/CE, en relación con la Directiva 2002/58/CE, de Privacidad y Comunicaciones Electrónicas.

Es por ello que, todos los Investigadores del Área de Salud Valladolid Este, que utilicen para sus proyectos de investigación aplicaciones móviles, deberán verificar que cumplen con la legislación sobre protección de datos y sobre privacidad de la información personal en el ámbito de las comunicaciones electrónicas, recogida en la Directiva 95/46/CE, traspuesta en España en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento que la desarrolla, en concordancia con la Directiva 2002/58/CE. **Ver ANEXO**.-

Por lo expuesto, cuando envíen Proyectos de Investigación para su valoración por este Comité, **deberán incluir entre la documentación**, un documento en el que se especifique " *que la aplicación cumple con los principios de protección de datos de carácter personal contemplados en la Ley Orgánica 15/1999, de 13 de diciembre, y en sus normas de desarrollo, así como con los postulados de la Directiva 95/46CE, sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y los de la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas".*

Aprobado en la Reunión del CEIC/CEIm Área de Salud Valladolid Este, el día 21 de Abril de 2016.

REQUISITOS QUE DEBEN CUMPLIR LOS PROYECTOS PRESENTADOS A ESTE CEIC/CEIm EN LOS QUE SE UTILICEN APLICACIONES MÓVILES

- La aplicación móvil ha de cumplir la directiva de protección de Datos 95/46, en relación con la Directiva 2002/58/CE de Privacidad y Comunicaciones Electrónicas.

- La aplicación móvil ha de cumplir con las directivas de seguridad SSL Directivas de Seguridad SSL:

- El protocolo SSL (Secure Sockets Layer) y su inmediato sustituto TLS (Transport Layer Security) son los protocolos que se utilizan con mayor frecuencia en entornos internet para asegurar las comunicaciones y los datos que se intercambian entre clientes y servidores. Son protocolos robustos que definen una serie de fases que deben ser implementadas por cada aplicación.
    - En el primer paso, el cliente inicia una conexión SSL con un servidor, en este paso, debe enviar al servidor web los settings de configuración que el Sistema-cliente soporta para el proceso de comunicación entre ambas partes, estos settings deben de incluir entre otros los siguientes:
        - Versión del protocolo SSL que el sistema-cliente soporta.
        - Algoritmos criptograficos que el sistema-cliente soporta para el cifrado de la comunicación (algoritmos de clave pública y clave privada).
    - Toda esta información es incluida en un mensaje que será enviado al servidor. Este tipo de mensaje pertenece a un sub-protocolo conocido como handshake
    - El sistema-cliente y el servidor ahora conocen cual será la configuración que se deberá emplear para establecer la conexión y ahora proceden a intercambiar sus correspondientes certificados (que dependen de los algoritmos de clave pública seleccionados anteriormente).

    - El siguiente paso, es la generación de la Master Secret que es generada tanto por el sistema-cliente como por el servidor, este proceso se realiza de forma paralela en el sistema-cliente y el servidor, el resultado final para ambos será el mismo
    - Con la Master Secret generada, tanto el sistema-cliente como el servidor comienzan a generar las session keys las cuales son claves simétricas usadas para cifrar y descifrar información intercambiada durante la sesión SSL y para verificar su integridad.
    - El handshake ha finalizado y la sesión SSL ahora puede comenzar, de ahora en adelante, tanto desde el sistema-cliente como desde el servidor, se utilizarán sus session keys generadas para cifrar y descifrar información que envían entre ellos, y para validar la integridad de los datos.

- Si los datos recogidos por el paciente en la aplicación móvil van a ser utilizados en estudios clínicos, se deberá.

  - Someter dicho estudio clínico con la información que en él se utilizará a dictamen de un CEIC/CEIm.

  - Incluir en la aplicación móvil un mensaje en el que el paciente acepte expresamente ceder esos datos clínicos debidamente anonimizados para la realización de estudios clínicos, sólo aquellos debidamente aprobados por un CEIC/CEIm, y para ninguna otra finalidad.