



PLATAFORMA TECNOLÓGICA ESPAÑOLA DE TECNOLOGÍAS PARA SEGURIDAD Y CONFIANZA

Ficha Descriptiva Grupo

"secSALUD"

2 de Octubre de 2009

Ficha de creación del grupo de trabajo

Nombre del nuevo grupo de trabajo: Privacidad y Seguridad en Salud

Acrónimo (nombre de referencia): secSalud

Nombre de la persona que propone: María Teresa Hurtado Mora

Datos de contacto

Entidad: TB-Solutions

Dirección: C/ Ronda del Canal Imperial de Aragón nº 14. CP 50197. Zaragoza

Teléfono: (+34) 976-70-16-00

Fax: (+34) 976-70-16-01

Email: hurtadom@tb-solutions.com

Descripción del grupo de trabajo:

La obligación de salvaguarda del secreto profesional en lo tocante a la información relativa a los pacientes en escenarios de Salud atañe no solamente a los médicos, sino también al resto de personal tanto sanitario como no sanitario que se relaciona con los pacientes o que accede a información concerniente a ellos. Esta obligación se encuentra reflejada en la normativa de protección de datos, en la normativa sanitaria e incluso el código penal.

Asimismo, las organizaciones sanitarias tienen entre sus cometidos el de preservar la integridad de la información clínica, así como su disponibilidad para cuando ésta sea necesaria, encontrándose accesible tan sólo para personas que se encuentren autorizadas para ello.

Con todo ello, el objetivo básico del grupo de trabajo Privacidad y Seguridad en Salud será el de la promoción de la investigación técnica dirigida a aumentar la seguridad de los sistemas de información y de comunicaciones aplicados a este escenario. Teniendo esto en cuenta, las actividades principales del presente Grupo de Trabajo se centrarán en alcanzar los siguientes objetivos maestros:

1. Realizar una gestión segura y eficiente de las **identidades** de los actores que hayan de acceder a registros de información de carácter sensible dentro de escenarios de Salud (por ejemplo, datos médicos, historias clínicas, etc.). Todo ello de cara a garantizar que, en todo momento, se tiene control sobre la persona o entidad que accede a la información, así como de que ésta posee los **permisos** y privilegios necesarios para ello.
2. Garantizar **la seguridad de la información intercambiada** entre los diferentes actores involucrados en el escenario de Salud (médicos y personal sanitario, personal de gestión, proveedores y/o consumidores de servicios de salud, etc.), una vez que éstos hayan sido identificados. Esta seguridad es

requerida habida cuenta de que la información intercambiada en dicho escenario, en la mayoría de los casos, es de carácter **sensible**.

Los objetivos anteriores están orientados a dotar a los escenarios de Salud de medidas de protección que permitan garantizar el acceso e intercambio seguros de la información de carácter sensible que se gestiona en dichos escenarios, avalando los siguientes aspectos de la misma:

- **La identificación fiable de la persona que accede a ella:** Se hace necesario identificar sin lugar a dudas a la persona que pretende acceder a información de carácter sensible. Esto se consigue mediante procesos de identificación (que permiten la presentación de credenciales a modo de “tarjetas de visita”) y de autorización (que permiten validar de manera fiable la autenticidad de las credenciales presentadas).
- **Su acceso seguro:** Una vez que la persona que pretende acceder a los datos de carácter sensible haya sido identificada, podrá concedérsele (o no) permiso para la ejecución de determinadas tareas sobre la misma. Es decir, deberá garantizarse que sólo acceda a la información quien esté autorizado para ello y únicamente para el uso para el que esté autorizado. Ello se consigue mediante procesos de autorización (control de acceso y asignación de perfiles y roles).
- **Su confidencialidad:** Que la información de carácter sensible se encuentre cifrada, de tal manera que su contenido pueda ser leído y entendido únicamente por el/los destinatario/s legítimo/s de la misma.
- **Su integridad:** Que la información no se haya transformado, ni accidental ni intencionadamente durante su almacenamiento o transporte.
- **Su disponibilidad:** Que la información pueda ser accedida y utilizada cuando ésta sea necesaria.
- **Su no repudio:** Que quien acceda o participe en la gestión de la información no pueda negar haberlo hecho.
- **Su auditoría:** Que la organización sanitaria pueda comprobar quién ha accedido a la información y en qué transacciones ha participado.
- **Disposiciones legales** en materia de seguridad, confidencialidad e historia clínica informatizada, así como otros aspectos técnicos y organizativos.

Como resultado de todo lo anterior, el Grupo de Trabajo de Privacidad y Seguridad en Salud se plantea crear unas bases que constituyan los pilares del estudio de **la gestión integral de la identidad digital en los escenarios de Salud**, así como para **garantizar la seguridad**, en los términos en los que ya se ha hecho mención, **de la información intercambiada** en los mismos.

Posibles aplicaciones:

La garantía de un tratamiento adecuado de la seguridad de los datos y comunicaciones en medicina abre un sinfín de posibilidades a nivel de interacción entre agentes y servicios, así como de facilidad y rapidez de gestión y consulta para trabajadores y pacientes.

Prácticamente cualquier campo de la medicina en el que se requiera acceso a archivos de información puede beneficiarse en gran medida de las garantías que proporciona un tratamiento seguro de los datos, por ejemplo, acceso a historiales clínicos por los facultativos o los pacientes, o una segregación de los datos útiles para el personal sanitario. Creación rápida, eficaz y real de informes de estado y aprovechamiento de los recursos médicos, facilitando una gestión óptima de los mismos en beneficio tanto de trabajadores como de pacientes y sus familiares. Localización, estado y evolución de pacientes en hospitales y residencias en tiempo real, gestión personalizada de las necesidades dietéticas, telemedicina, servicios asistenciales, preventivos e informativos...

En general, no hay área de la medicina que no se pueda ver beneficiada en calidad de servicio, confiabilidad y facilidad de uso mediante un tratamiento adecuado de la información.

Con todo lo anterior, un potencial escenario de aplicación de las actividades desarrolladas en el Grupo de Trabajo de Privacidad y Seguridad en Salud será la **informatización segura de la historia clínica**. La historia clínica informatizada ha supuesto la introducción de las tecnologías de la información en el núcleo de la actividad sanitaria. Este proceso ha traído consigo la integración de la información dispersa en varias bases de datos de centros sanitarios, como las de laboratorios clínicos, programas de admisión, etc. El siguiente paso ha sido la integración de la información clínica, correspondiente a una persona, que se encontraba ubicada en todos los centros sanitarios en que hubiera sido atendida.

Evidentemente, la historia clínica contiene información del ámbito de la intimidad de las personas. Así pues, su informatización para hacer posible el acceso a los datos en ella contenidos desde otros lugares en los que pueda ser necesario para atender al paciente, así como la creación de bases de datos centralizadas generan inquietud por la seguridad de dicha información entre los médicos, así como entre los pacientes. Los primeros se preguntan si se puede garantizar que esos datos no llegarán a manos de quien pueda utilizarlos con otros fines que aquellos para los que fueron recogidos: diagnosticar y curar a los pacientes, mientras que los segundos se preocupan acerca de quiénes tendrán a su disposición sus datos médicos de carácter personal. Por todo ello, se hace necesario el adoptar medidas que permitan garantizar la seguridad en los accesos e intercambios de este tipo de información, siendo éstas las actividades principales del presente Grupo de Trabajo.

Otra posible aplicación de las actividades del presente Grupo de Trabajo tendrá lugar en el **escenario del hogar**, con aplicaciones de tele-medicina y tele-asistencia, monitorización, sensorización, hospital virtual, etc. Estas actividades se centrarán en el aseguramiento de las tecnologías de la información que posibiliten herramientas de apoyo orientadas a facilitar la vida independiente de las personas mayores en sus viviendas, aun encontrándose en situación de dependencia. Dichas herramientas implicarán necesariamente el intercambio de información entre los diferentes actores involucrados en los servicios que se presten (usuarios finales, familiares, proveedores de servicios de salud, etc.).

Así pues, antes de que estas soluciones puedan ser adoptadas en la práctica, se deberán tomar en consideración los aspectos de la seguridad de esa información, así como de quién accede a ella y para qué. El éxito de las iniciativas en este sector dependerá en gran medida de que se proporcione un intercambio seguro de la información personal, y de que se preserve la privacidad de dicha información. La

privacidad no implica únicamente la confidencialidad de los datos transmitidos, sino también los conceptos de control, autonomía e integridad. Los usuarios tienen derecho a controlar qué información debe permanecer en su propia casa, y cuál debe ser enviada a otros lugares. Deben además tener la capacidad de controlar para qué propósito se recoge, almacena y transmite la información.

Otra potencial línea de actuación en la que el presente Grupo de Trabajo podría desarrollar su actividad de aplicación de las tecnologías de identificación, autenticación y autorización, así como de los procedimientos de protección de la seguridad de los datos e infraestructuras en el escenario de Salud, sería la de la **trazabilidad de personas y objetos**. Ésta línea permitiría, por ejemplo, acometer la localización de pacientes en tiempo real dentro de un recinto hospitalario durante un proceso asistencial, vinculando los datos de localización a un identificador único asociado al paciente que no revelara su identidad (preservando de esta manera su derecho fundamental a la intimidad).

Estado actual del sector de aplicación:

La situación actual del sector de Salud en lo que se refiere tanto a privacidad como a seguridad de la información intercambiada, resulta bastante precaria. Apenas existe seguridad de acceso a la información y en aquellos lugares donde se controla de alguna manera, no existe garantía de que esa información no haya sido manipulada (integridad) o se esté suministrando con alguna política de gestión de permisos, a los usuarios que la consultan (no todo el mundo debería tener acceso a los mismos datos).

Asimismo la posibilidad de incorporar cierta información de manera digital a la historia clínica de un paciente posibilitaría reducir en gran medida el coste de gestión de dicha información al ganar tanto en espacio como en tiempo. Sin embargo, estas mejoras llevarían consigo el incremento de la seguridad aplicable a las mismas en pos de una tranquilidad para los pacientes (que tendrían constancia de que sus datos no circulan sin seguridad alguna o en manos de quien no deba) y un cumplimiento del reglamento ya citado anteriormente.

Otros comentarios:

La tendencia actual es el acceso a la información clínica desde cualquier momento y lugar en el que pueda ser necesario para la debida atención del paciente, con independencia de en qué centro sanitario haya sido generada esa información.

Hoy en día, existe pues una directriz muy marcada hacia la **provisión de servicios sanitarios por múltiples canales**. Ello hace necesario disponer de procedimientos de seguridad adaptables, que puedan aplicarse a un número creciente y cambiante de canales de intercambio de información (PC, terminal móvil, TDT, etc.), así como a los portales de Salud multicanal que se ofrecen al usuario.

El grupo SecSALUD es un **grupo mixto** de las Plataformas eSEC y eVIA.