Global Information Assurance Certification Paper

Análisis de la Implementación de Lectores de Huella Dactilar y Firmas Digitales en los Registros de un Software de Historia Clínica Electrónica en Colombia

GIAC Security Essentials
Certificacion (GSEC)
Practical Assignment

Option 2 - Case Study in
Information Security

Submitted by: Alejandro Forero R.
Location: Local Mentor en Bogotá (Colombia)

Tabla de Contenido

Introducción

La implementación de nuevas tecnologías en la medicina ha permitido en el entorno Colombiano la introducción de los sistemas digitales de registro y control médico/administrativo como lo es la Historia Clínica Electrónica (HCE). Sin embargo las inquietudes de seguridad y la carencia de una legislación particular al respecto que determine los parámetros bajo los cuales el acceso a la información debe ser preservada, han demandado que estos sistemas sean complementados por medio de aplicaciones específicas de validación y control de acceso a la información médica que garanticen al personal médico y al paciente la seguridad que esta no será accesada ni manipulada por personal diferente al autorizado.

Los desarrollos tecnológicos recientes han permitido definir e implementar un sistema de historia clínica digital, que soporte la actividad médica y paramédica de todo un centro hospitalario, este desarrollo ha evidenciado la necesidad de seguridad y validación de acceso a la información medico-asistencial que tiene el personal de la institución; generando así la necesidad de soluciones novedosas para los nuevos problemas planteados. En donde una de estas soluciones es la generación una herramienta software basada en sistemas de identificación biométricos como el lector de huella dactilar y firma digital (mediante certificados digitales) de los registros generados dentro de la Historia Clínica que brindan un alto nivel de seguridad al manejo de la información médica, permitiendo aprovechar la flexibilidad del entorno que ofrecen las clínicas digitales.

Antes

Situación de Seguridad Actual

El desarrollo y evolución de las tecnologías de la información ha llevado a la aparición de un gran número de aplicaciones informáticas en los diferentes países, para ayuda en el diagnóstico, tratamiento y gestión de los pacientes como no lo indica Javier Carnicero Giménez de Azcárate:

> *"Durante los últimos años se han desarrollado soluciones informáticas para la historia clínica de atención primaria y especializada, así como para integrar la información de los sistemas departamentales. En el momento actual todos los servicios de salud de nuestro sistema sanitario se encuentran en fase de análisis, desarrollo o despliegue de sistemas de información clínica, que contemplan soluciones para la historia clínica de atención primaria, especializada o ambas". [1]*

Estas aplicaciones han permitido la evolución del concepto tradicional de historia clínica en papel (como documento exclusivamente médico, limitado a recoger información de un proceso concreto, habitualmente de enfermedad, en un tiempo y lugar específico) hacia un nuevo concepto de HCE capaz de integrar toda la información referida al estado de salud de una persona, acumulada a lo largo de la vida del individuo, y generada por todos los responsables de la atención en salud que han intervenido en los diferentes procesos asistenciales, como lo indica J*osé Luis Monteagudo, j*efe del Area de Proyectos Internacionales del Instituto de Salud Carlos III, quien ha participado en una jornada sobre documentación médica que se ha celebrado en la Fundación Hospital de Alcorcón, de Madrid*:*

> *"Quienes otorgan una mayor significación a la informática en el ámbito de la medicina piensan que en el futuro habrá un buen número de instrumentos que facilitarán el trabajo de los profesionales sanitarios. Pero el futuro más inmediato ha de pasar por el desarrollo de una buena historia clínica informatizada, puesto que es el elemento clave de cualquier arquitectura de sistemas de información". [2]*

Actualmente un gran número de centros de atención médica en Colombia, por no decir que todos, tienden a contar al interior con su propio sistema de información hospitalario completamente "informatizado", así como de una HCE que contenga todos los elementos tradicionales (documentos, ordenes, imágenes, pruebas / resultados, entre otros), posibilitando el acceso a la información por parte de un gran número de profesionales médicos, asistenciales y administrativos de la institución que cumpla con las reglamentaciones del ley para tal fin. Así también como se ha ampliado la infraestructura tecnológica dentro de las instituciones de salud, posibilitando el acceso a la información médica desde diferentes dispositivos como Pc's, TABLET Pc y las PDA's, asiendo posible acceder a la información de la HCE desde mucho lugares a la vez; a si como el rápido aumento del número de PC que están siendo utilizados en las instituciones de salud en los últimos años, en especial aquello para el área médico asistencial.

Descripción del Problema

En las instituciones de salud la toma de decisiones tienen como soporte la información aportada por los profesionales de la salud; además son estos los encargados de decidir sobre la utilización de recursos diagnósticos y terapéuticos; haciendo que la posibilidad de poder almacenar en forma digital los registros médicos de los pacientes representa una magnifica oportunidad para el acceso y manejo de la información confiable rápidamente.

El avance tecnológico de los ultimo años ha permitido la aparición de un gran número de herramientas de registro electrónico de soporte clínico y respaldo a los profesionales de la salud en la entrega oportuna y segura de datos pertinentes, mientras se encargan del cuidado de la salud del paciente, permitiéndoles a estos profesionales documentar sus propias observaciones, acciones e instrucciones, y ayudando a los usuarios no clínicos o personas no involucradas directamente con el cuidado del paciente con la evaluación de elementos administrativos de la institución. Este desarrollo ha aportado un gran caudal de conocimientos al respecto, pero también han puesto de manifiesto una serie de requerimiento relacionados con algunos inconvenientes de seguridad[1] presente en el sistema, que deben tenerse en cuenta a la hora de llevar a cabo cualquier implementación de una herramienta electrónica para la facilitar la gestión médico asistencial en las instituciones de salud [3].

Cualquier herramienta electrónica o sistema de información que pretenda soportar y complementar la gestión clínica de las instituciones de salud debe tener una especial atención con la amenaza de seguridad del sistema sobre la autenticidad, confidencialidad e Integridad de la información del paciente (Quien, cuando y por que debe o puede acceder esta información) [4], como lo resalta Javier Carnicero Jiménez:

> *"Los aspectos de seguridad y confidencialidad, éticos, legales y técnicos, resultan de la mayor importancia, puesto que la información clínica es muy sensible y además se aspira a que los profesionales, tanto sanitarios como no sanitarios, que estén implicados en la asistencia al paciente, puedan acceder a ella en cualquier momento y lugar en que este sea atendido". [1]*

Otro aspecto importante a tener dentro en el sistema de seguridad de la HCE es el que destaca el secretario general de la Organización Médica Colegial (OMC) de españa, Juan José Rodríguez-Sendín [5]:

> *"El peligro de este nuevo método informatizado, ya que la concentración de la información estimula y facilita las intromisiones interesadas y multiplica el alcance de los errores y accidentes inevitables, y que tendrían consecuencias irreversibles para los pacientes".*

Además, critica que dentro de la instiruciones y en el entorno:

[1] Entendiendo aqui por seguridad los siguientes aspectos: Autenticidad (saber quién genera la información); integridad (estar seguro que la información no ha sido alterada); confidencialidad (que nadie más que el personal autorizado tenga acceso a los datos), y no repudio (no se puede negar que se ha genera la información porque consta de la firma.

"no ha habido la necesaria claridad y transparencia en la puesta en marcha de este sistema tanto para los profesionales sanitarios, como para los ciudadanos".

Riesgos Actuales

Antes de la implantación de este proyecto el sistema de seguridad del software HCE que se manejaba hasta ese momento, estaba basado en el tradicional modelo seguridad USUARIO + CLAVE. Este modelo no garantiza por completo la confidencialidad e Integridad de la información médica, siendo altamente susceptible a problemas de seguridad, debido a prestamos de claves entre el personal de la institución, usurpación de identidad y Keyloggers que permiten que la historia clínica de un paciente pueda ser vista y/o modificada por personal no autorizado para tal fin, generando los siguientes riesgos:

- Modificaciones y/o pérdida de la información medica del paciente registrada en el sistema.

- Acceso no autorizado a la información del paciente e incumplimiento de la ley de confiabilidad de la información del paciente, Violación del "Secreto Médico[2]"

Impacto de la capacitación de SANS en la situación

Por medio de la capacitación recibida de SANS, se pudo apreciar claramente la difusión que han tenido las aplicaciones de seguridad, que han permitido cada vez más el desarrollo y evolución de soluciones innovadoras, que integran diferentes tipos de identificación biométricas a los sistemas de acceso críticos en diferentes organizaciones tales como bancos, hoteles, aeropuertos, clínicas, entre otras.

La introducción de estas tecnologías en el sector de la salud se presenta como una necesidad, debido a su gran potencialidad para de generar un aporte de alto impacto en el mantenimiento de la seguridad (confidencialidad e integridad de la información médica) del sistema; permitiendo garantizar la identidad del médico y en general de las diferentes personas que deben y pueden tener acceso a la información médica de los pacientes allí registrada.

[2] El secreto del médico, inherente al ejercicio de la profesión es un derecho del paciente que obliga a cualquier médico en su ejercicio y que no se extingue por el fallecimiento del paciente.

Durante

Solución Propuesta

Como primer paso se conformo un grupo interdisciplinario compuesto por personal administrativo, médicos, asistencial, abogados, ingenieros de sistemas y técnicos de la Institución para analizar la problemática y determinar el plan de acción a seguir para eliminar o minimizar los riesgo que se estaba presentando en cuanto a la seguridad de la información médico – asistencial en la HCE; buscando alcanzar un equilibrio entre accesibilidad y seguridad del sistema, de forma que éste no colapse, haciendo que no estén disponibles.

Como resultado de este análisis, se determinó implementar dentro del software de Historia Clínica Electrónica dos desarrollos fundamentales para robustecer el control al acceso de la información y la integridad de los registros médicos: Lectores de huella dactilar y firmas digitales mediante certificados de seguridad avalados por una entidad certificadora legal válida en Colombia.

La incorporación de estas tecnologías en la HCE permitirá asegura que la identidad del personal que accede y modifica la información medica es aquella que esta autorizado y cuenta con los permisos para hacerlo; además permitirá firmar digitalmente los documentos generados por el personal médico de la institución, asegurando la integridad de los documentos generados por el sistema.

Implementación de la solución

Para implementar la solución propuesta dentro del software de HCE fue necesario evaluar las diferentes alternativas en lo referente a diferentes marcas de los lectores de huella disponibles en el mercado y seleccionar a un proveedor con reconocimiento mundial en el área de desarrollo tecnológico, el cual facilitó el Software Development Kit (SDK) del lector de huellas para desarrollar nuestra propia rutina que fue totalmente integrada a la HCE.

Figura 1. Lector de huella digital.

Para lo cual fue necesario el desarrollo de una serie de librerías que permitieran el manejo de las siguientes funciones:

- Leer la huella del dedo en el dispositivo en escalas de grises
- Generar la imagen de la huella dactilar para poderla visualizar en pantalla del PC
- Generar la plantilla correspondiente a la huella dactilar y almacenar la plantilla en una Base de Datos (BD)
- Grabar los datos de la plantilla almacenados en BD en la memoria del dispositivo al lector de huella dactilar
- Detectar si hay dedo sobre el dispositivo
- Leer la huella del dispositivo y compararla con la plantilla almacenada en la memoria del mismo.

En cuanto implementación de los certificados digitales en la HCE, se optó por trabajar con la entidad certificadora en Colombia, siguiendo los parámetros planteados en los decretos 1995 de 1.999 (Ley de Archivo General de la república) y la ley 527 del mismo año (Ley de Comercio Electrónico). Esta entidad entregó el dispositivo Token key[3] (ikey) con su correspondiente PIN de seguridad y los respectivos drivers; el cual contiene la firma digital respaldada por la entidad certificadora.

Figura 2. Token key. http://www.safenet-inc.com/

Para incorporar esta tecnología fue necesario capacitar a pequeño grupo de ingenieros de sistemas sobre el uso de este dispositivo y sobre las reglamentaciones existentes al respecto en Colombia. Este grupo de profesionales fueron los encargados de llevar a cabo el desarrollo y ejecución

[3] La token ikey consiste en microprocesador con una memoria y un controlador USB todo dentro de un dispositivo bastante pequeño para almacenar el certificado digital. Este dispositivo proporciona capacidades de almacenaje altamente confiables.

del proyecto de integración de esta tecnología a la HCE, en donde fue necesario incorporar librerías de Microsoft (cryptoapi) para el manejo de certificados digitales al software de HCE. Y se implemento dentro de la HCE las siguientes funciones para incorporar la firma digital:

- Firma de procedimientos médicos.
- Generación de Documentos médicos y administrativos en formato ELECTRONICO firmados digitalmente.
- Verificar la firma digital del documento corresponde al usuario registrado en el mismo.
- Permitir la protección de la información por medio de encriptación de los datos usando llave pública y llave privada.

Después

Al implementar esta solución fue necesario realizar algunos cambios en la forma de asignar los derechos a los usuarios de la Historia Clínica Electrónica, generando a su vez un cambio en la cultura del manejo de la información médico asistencial. Estos cambios comprenden también a la forma de ingresar a la HCE por parte del personal de la institución y en la generación de documentos, que se harán con firma digital del usuario que los genera.

Para el proceso de acceso a la HCE el usuario registrado en el sistema debe colocar su nombre de usuario y el sistema le solicitará la huella según este configurado el perfil del usuario. Seguidamente el software carga la plantilla correspondiente a la huella del usuario que se encuentra en la BD del sistema en la memoria de dispositivo (este dispositivo puede soportar hasta mil plantillas de huella, además de datos del nombre, el rol y hasta 16 caracteres adicionales para cada una de las plantillas). Cuando el sistema esta configurado para la huella, él le solicita al usuario colocar su dedo en el lector de huella dactilar, para proceder a leer la huella, generar la plantilla de la misma y compararla con la que tiene almacenada en la memoria del dispositivo, asociada a ese usuario. Si las plantillas corresponden entre si; y existe además un 90% de similitud entre las misma, se da acceso al usuario al sistema, pero si este porcentaje es menor se indica al usuario que debe captura la huella de nuevo; por otro lado si en el software detecta que la huella detectada no corresponde a la que tiene almacenada para el usuario, no le permite el acceso a la HCE a ese usuario.

El proceso de incorporación de la firma digital en un documento médico, inicia cuando la persona autorizada para ingresar a la HCE conecta la ikey que contiene su correspondiente firma digital a la terminal de trabajo (Pc), e ingresa

el Pin de la ikey, para poder generar el documento que contenga la firma digital correspondiente al certificado de la ikey del usuario.

Validación y Prueba de la Solución

Al momento de la implantación de esta solución fue preciso realizar una serie de pruebas de validación sobre su funcionamiento y desempeño del sistema, por lo cual fue necesario efectuar algunos ajustes en el desempeño y facilidad de uso de software; teniendo en cuenta siempre que la implementación de mecanismo para controlar la seguridad e integridad de la información requiere la mayoría de las veces el sacrificio de algo de comodidad en el uso del software.

Aseguramiento de los Riesgos

No obstante la implementación de esta solución dentro del software de HCE, se sigue planteando la pequeña factibilidad de vulnerabilidad de la seguridad del sistema, por las características innatas del dispositivo lector de huella dactilar; debido a que este dispositivo no es 100% seguro contemplando la posibilidad de un error en un millón.

Por otra parte en el manejo de la firma digital, cabe la posibilidad que otra persona conozca el Pin del ikey y pueda ser usada por esta persona con o sin consentimiento del propietario de la misma.

Estos riesgos no representan una muy pequeña proporción en la vulnerabilidad de la seguridad del sistema para ser considerados como riesgos con un nivel de incidencia (frecuencia e impacto del riesgo) a considerar en la seguridad de la información de la HCE.

Conclusión

El actual contexto del manejo de la información favorece la evolución de los sistemas de seguridad, debido en su mayoría a la gran velocidad con que evolucionan tecnologías de la información; como lo es la incorporación de sistemas de identificación biométrica, el cifrado de información, firmas digitales, entre otros; además del desarrollo estándares de seguridad de aceptación mundial. En este sentido cabe destacar el impacto que el manejo de la seguridad informática ha generado, en el aumento de la tranquilidad y seguridad que tienen los usuarios de estas tecnologías, respecto a que sus datos estén almacenados en medios electrónicos seguros y confiables, generando a su vez una alto nivel de confianza en las mismas.

La sociedad de la información y la revolución de las tecnologías de la

información y de las comunicaciones han influido en el ejercicio de la medicina y demás profesiones sanitarias, y en la transformación de la historia clínica. En donde la información documentación clínica digitalizada no supone menos garantías de seguridad y confidencialidad que la documentación en papel, pero también exige establecer procedimientos y planes que garanticen esa confidencialidad y seguridad. Dentro de este argumento uno de los más importantes derechos del paciente es la confidencialidad de la información que ha facilitado a su médico. Y una de las obligaciones más importantes del médico y del resto de profesionales sanitarios o no, es garantizar ese secreto. Los servicios sanitarios deben arbitrar procedimientos que garanticen la seguridad y la confidencialidad de la información clínica.

El desarrollo e implementación de la solución aquí planteada permitió reforzar el sistema de seguridad de la HCE, contribuyendo a eliminar casi en su totalidad los riesgos detectados en cuanto a la seguridad de acceso y manejo de la información médica de la HCE, aumentando así la confianza de los pacientes de que sus datos están en manos seguras al interior de la institución.

Dentro de este desarrollo y evolución del sistema de seguridad del software de HCE, el siguiente paso necesario corresponde al fortalecimiento del sistema de seguridad, el cual implica conocer modelos de seguridad de la información reconocido como el modelo del Acta de Responsabilidad y Portabilidad de los Seguros de Salud (HIPAA, por sus siglas en ingles Health Information Patient Accountability Act)], y buscar la implementación de este modelo en la institución de cuerdo al entorno nacional.

References

[1] De la Historia Clínica a la Historia de Salud Electrónica. La historia clínica en la era del conocimiento. Javier Carnicero Giménez de Azcárate. www.seis.es/informes/2003/PDF/CAPITULO2.pdf.

[2] La historia clínica electrónica es el eje del sistema de información. *José Luis Monteagudo. http://www.diariomedico.com/gestion/ges240599combis.html*

[3] http://www.jrc.es/home/report/spanish/articles/vol81/ICT3S816.htm; Andreas Litgvoet, RAND Europa.

[4] http://www.biocom.com/informatica_medica/legalrec_firma_digital.html; www.biocom.com

[5] La OMC alerta sobre los "graves" riesgos de la historia clínica centralizada y exige una legislación propia, www.Diariomediaco.com, 04 de febrero de 2005.