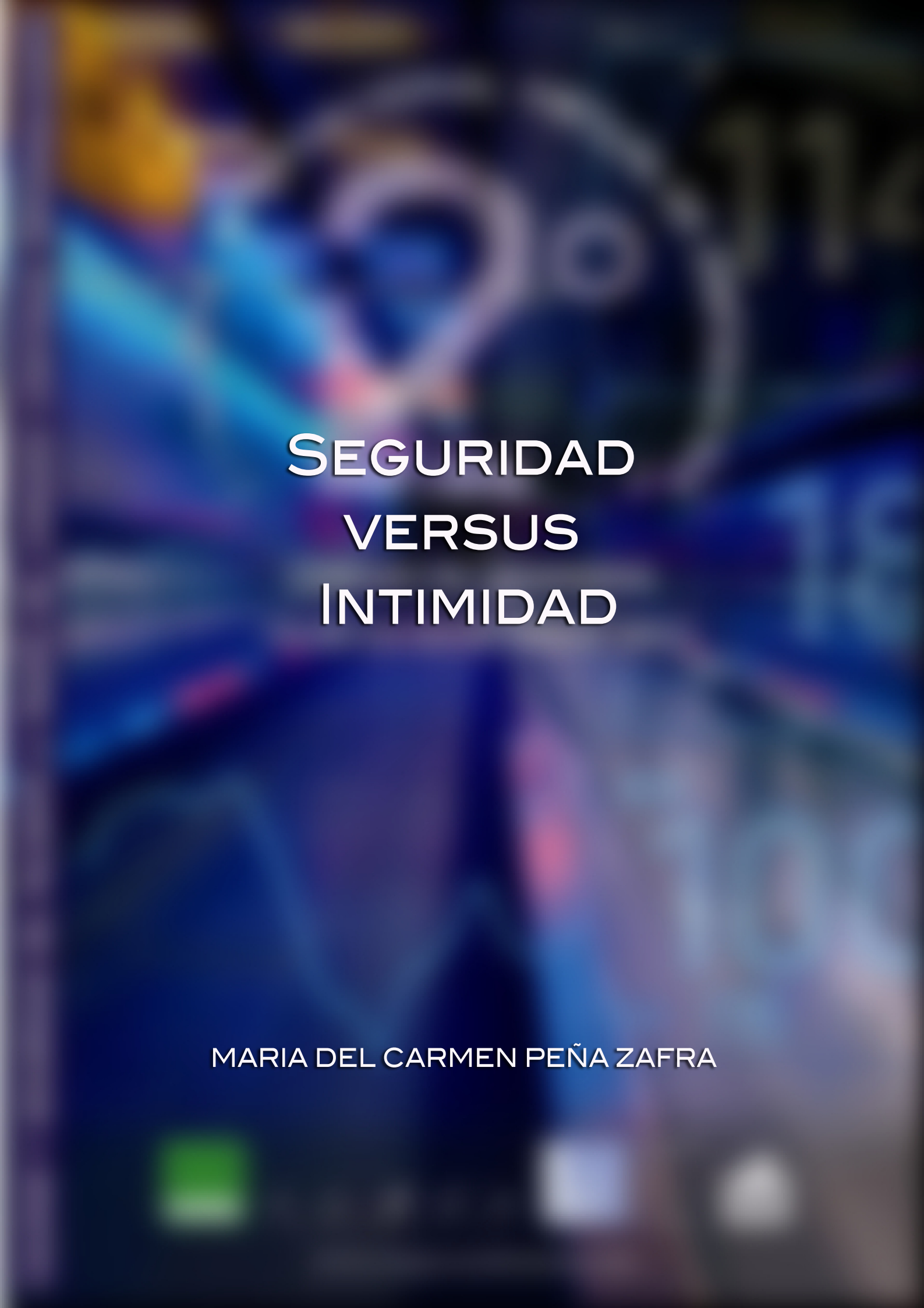

Seguridad versus Intimidad

MARIA DEL CARMEN PEÑA ZAFRA

II CONGRESO INTERNACIONAL VIRTUAL DE ENFERMERIA CIUDAD DE GRANADA

"Calidad y seguridad del paciente a través del cuidado continuo personalizado"

Seguridad versus Intimidad

Autor principal MARIA DEL CARMEN PEÑA ZAFRA

CoAutor 1

CoAutor 2

Área Temática PROYECTOS EUROPEOS E IBEROAMERICANOS EN LA GESTIÓN DE RIESGOS Y MEJORA DE LA SEGURIDAD DEL

Palabras clave Seguridad computacional Administración de la seguridad Confidencialidad Aplicación de la ley

» Resumen

Pretendo llamar a la reflexión sobre la importancia de la seguridad de los sistemas de información y la calidad en el tratamiento de los datos de nuestros pacientes. A continuación he tratado de buscar una solución a los problemas expuestos, haciendo relevante la importancia que una legislación eficaz en materia de privacidad y el cumplimiento de la misma tienen para las personas y entidades. Por otro lado hago una reflexión sobre lo que considero sería una buena solución a los problemas expuestos: el cloud computing.

» Contexto de partida. Antecedentes. Experiencias previas. ¿Dónde se realizó el trabajo? ¿En qué tipo de organización o departamento? ¿Cómo surge? ¿Hay experiencias previas en el área desarrollada?

Todos recordamos algunas de las últimas catástrofes mundiales: atentados terroristas contra el World Trade Center en Estados Unidos, incendio de la Torre Windsor en Madrid, maremoto de Sumatra, etc. También podemos leer titulares de prensa recientes como El temblor, que también se ha sentido en Cuba y República Dominicana, ha provocado el derrumbe de un hospital y otros edificios, La ciudad portuaria de Minami Sanriku (Japón) casi ha desaparecido. Sólo el hospital, una construcción de cinco pisos, y unos pocos edificios más, siguen en pie.

He reflejado estas noticias para llamar la atención sobre la destrucción de información vital para la continuidad de empresas, hospitales, etc., pero además de ello cabría plantearse ¿qué coste humano y económico tiene la perdida de toda esta información?, ¿cómo podemos evitarla?, y no me refiero a la catástrofe natural, que es inevitable pero si a lo que podemos hacer para disminuir sus consecuencias y todavía más importante, reducir el coste de vidas humanas, el dolor de los pacientes, y los sacrificios innecesarios que tan dolorosas perdidas ocasionan.

La lectura de artículos sobre la dificultad de conocer el número de desaparecidos, la destrucción de hospitales o la desaparición de varios registros oficiales de filiación (lo que supone que entre otras cosas no se pueda saber ni quienes, ni cuantas son las personas que buscamos), nos da una idea del problema que se nos puede presentar, por culpa, al fin y al cabo, de una mala gestión de la información de datos de carácter personal, Esto me hizo recapacitar sobre lo que podría ocurrir con la perdida de la información de los sistemas de salud y sobre la importancia de tener en puerto seguro la información sanitaria de carácter personal de nuestros pacientes y la seguridad de los mismos, junto con la calidad en su recogida y tratamiento, como un desempeño profesional que en todo momento debemos de tener presente.

» Descripción del problema. ¿Sobre qué necesidades o problemáticas del contexto pretendía actuar el proyecto? ¿Cómo se analizaron las causas de esos problemas? ¿Qué tipo de intervención se realizó? ¿Cómo se cuantificó el problema?

La O.M.S., en 2007, lanzó nueve soluciones para la seguridad del paciente, dirigidas a evitar los problemas relacionados con ella, y enfocadas a ayudar a reformular los procedimientos de asistencia al enfermo haciéndolos más seguros:

1. Medicamentos de aspecto o nombre parecidos.
2. Identificación de pacientes.
3. Comunicación durante el traspaso de pacientes.
4. Realización del procedimiento correcto en el lugar del cuerpo correcto.
5. Control de las soluciones concentradas de electrólitos.
6. Asegurar la precisión de la medicación en las transiciones asistenciales.
7. Evitar los errores de conexión de catéteres y tubos.
8. Usar una sola vez los dispositivos de inyección.
9. Mejorar la higiene de las manos para prevenir las infecciones asociadas a la atención de salud.

Sin considerar las nueve soluciones como cerradas, yo entiendo, que deben ser una guía desde la que podamos partir como una serie de premisas básicas asistenciales que a fecha de hoy se pueden comprobar como eficaces. Pero quiero hacer un planteamiento diferente de la seguridad del paciente, aunque complementando lo anterior e intentando responder a la siguiente pregunta ¿Cómo se puede ver afectada, si se realiza un erróneo tratamiento de los datos de carácter personal, la intimidad del paciente y su seguridad?

No cabe duda que la tendencia de futuro, presente hoy ya en algunos países, es la atención personalizada, monitorizando los datos sanitarios, por medio de las tecnologías de la información y la comunicación (T.I.C.), que pueden dotar a los sistemas sanitarios de mayor eficacia y capacidad de respuesta. Esta claro que la masificación de la ingente cantidad de datos requeridos para cada paciente, exigirá bases de datos enormes, que por otro lado requerirán de un tratamiento de las mismos de forma inteligente; es aquí donde la seguridad se convierte para el profesional en un añadido muy importante dentro de su desempeño laboral y para los centros sanitarios, una forma de cumplir eficientemente con la tan demandada responsabilidad social corporativa.

La legislación actual de la Unión Europea, están potenciando insistentemente, todo lo referente a la salud y la seguridad en el trabajo, así como la protección de los datos de carácter personal y la seguridad de los mismos, especialmente los relacionados con la salud, donde se exige que los sistemas que los van a tratar estén dotados de un nivel de seguridad alto, así como los lugares donde se van a ubicar. Si nos planteáramos lo ocurrido estos días en Japón, desde un punto de vista sanitario/empresarial, y supusiéramos que los centros sanitarios se hubieran visto afectados en sus sistemas de tratamiento de datos, destrucción de los mismos, accesos imposibles por destrozos materiales, y un largo etc., y si además lo relacionáramos a nivel empresarial con lo ocurrido tras el 11 de septiembre con las torres gemelas del World Trade Center de Nueva York, donde desaparecieron muchas empresas por no poder dar continuidad al negocio, al haber perdido los datos de sus clientes, especialmente los de carácter personal y carecer de copias de seguridad de los mismos, podríamos hacer una reflexión de la importancia de una eficaz gestión de la seguridad de la información, y de la gran complicación que conllevaría realizar una atención sanitaria segura y eficaz. En estos casos, es donde hay que preguntarse ¿seguridad o intimidad? Por lo tanto yo añadiría una décima solución a las propuestas por la O.M.S.: Seguridad en los sistemas de gestión de la información de los datos de carácter personal de los pacientes.

» Soluciones aportadas / Viabilidad / Aplicabilidad. Coste-Beneficio. ¿Cuáles fueron los efectos y cómo se midieron? ¿Hasta qué punto las soluciones aportadas resolvieron el problema?

Debemos atender a la seguridad y calidad en la gestión de los datos de nuestros pacientes, como una parte inseparable de ese todo que es la seguridad y calidad en sentido general. Teniendo en cuenta la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos (L.O.P.D.) base de nuestra legislación en materia de privacidad, en lo concerniente a los datos de carácter personal y a los considerados datos especialmente protegidos, sabemos que los datos de carácter personal que hagan referencia al origen racial, a la salud o a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente. Con algunas excepciones, como son: salvaguardar el interés vital del afectado o de otra persona, cuando resulten necesarios para la prevención o para el diagnostico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por personal sanitario sujeto al secreto profesional o por otra persona sujeta a otra obligación equivalente de secreto.

Quisiera hacer una consideración, si entrar en más detalle, sobre lo que el apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, viene a definir como dato relativo a la salud, las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. Este tipo de datos no se refiere exclusivamente a las historias clínicas, que ya tienen además su regulación específica (Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derecho y obligaciones en materia de información y documentación clínica), si no también a la que se puede encontrar en ficheros, automatizados o no, de recursos humanos. No es baladí recordar que no solo los profesionales de la sanidad tratan datos de salud.

Por otro lado y en relación a la L.O.P.D., y muy especialmente en lo relativo al principio de seguridad, tendremos en cuenta lo que impone a todas las entidades el art. 9 de la misma, obligándole a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal a los que accedan en su actividad diaria, con el fin de evitar su alteración, perdida, tratamiento o acceso no autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Esta última línea es de vital importancia y justifica que las entidades de toda índole contemple, como prioritario, un adecuado plan de continuidad de negocio, entendiendo este en su acepción más general. Actuar así, es ser socialmente responsable.

De lo anterior se desprende que un adecuado tratamiento de los datos de salud de nuestros pacientes, considerados por toda la normativa en materia de protección de datos, como de nivel alto, requerirán para ser seguros y de calidad, una serie de medidas de seguridad adecuadas:
1. Existencia de documentos de seguridad, en los que se recojan las políticas, estándares y medidas de seguridad.
2. Controles de acceso a través de medios de identificación y autenticación.
3. Control de la gestión de los soportes mediante inventarios y registro de entradas y salidas.
3. Realización de copias de seguridad y su almacenamiento en un lugar distinto al que se encuentran los sistemas de información.
4. Cifrado de comunicaciones y soportes, y un largo etcétera.

Haremos hincapié en la importancia del penúltimo punto anterior y fundamentalmente, contestar a las preguntas que nos hacíamos en la introducción. Para ello quiero enfocar las diferentes soluciones o las posibles respuestas, sobre el concepto cloud computing, conocido como nube. El futuro de la información, es sin duda ella. Podremos a través de Internet, compartir un enorme volumen de información y gestionarlo más fácilmente. En ella podremos tener para siempre nuestros documentos, agendas, correos, fotos, etc., acceder a ellos desde cualquier sistema con conexión a internet, y garantizar su privacidad y seguridad. Con ella evitaríamos la grave perdida de información valiosa.

Comparativamente hablando, entre los servicios de almacenamiento de datos actuales y los que proporciona la nube, ésta tiene unas ventajas importantes que serían: la fragmentación y dispersión de datos, la replicación automatizada, la provisión de zonas de datos (hospitales, comunidades médicas, países etc.), permitir el cifrado tanto en reposo como en tránsito de los mismos y la retención automatizada de datos.

Si un eficaz plan de continuidad, pasa por garantizar y conservar el valor de la información, parece evidente que la misma debe de estar alejada de todo tipo de posibles catástrofes. En este sentido esta claro que es necesario y socialmente responsable poseer una información que sea redundante, y que la distancia en la cual se ubique la copia o copias de la original este fuera de cualquier posible destrucción.

» Barreras detectadas durante el desarrollo.

Expuestas las principales ventajas, que de cara a la atención sanitaria, comportaría la nube, quisiera hacer una reflexión sobre los actuales inconvenientes: nos podríamos encontrar sin acceso a Internet, o con uno limitado, en este caso se perjudicaría la disponibilidad en relación a la seguridad; la no portabilidad de aplicaciones entre diferentes sistemas o plataformas, como en el caso anterior seria un perjuicio a efectos de disponibilidad pero no de seguridad.

Si quisiera llamar, de forma significativa, la atención sobre el que considero actualmente el primero y más urgente de los problemas, la protección de la seguridad y la privacidad de los datos y la posible perdida de control que sobre los mismos pudiera acaecer. El cloud computing puede presentar algunos fallos en lo referente a la gestión y control del almacenamiento de los datos, que pueden hacer que se vean comprometidos como, por ejemplo, una exposición de los datos a intromisiones de hackers, o el hecho de que algunos gobiernos no

tengan una eficaz legislación en materia de privacidad.

Por lo tanto habrá que dotar progresivamente a la nube de medios que la hagan lo más segura posible. Esta debe ser la tendencia de una tecnología que considero es imparable.

» Oportunidad de participación del paciente y familia.

Si pensamos en la web 2.0, también conocida como la web social, casi todos estamos conectados a alguna red social, en la que compartimos información personal, videos, fotos, etc. Comprenderemos que no es tan difícil disponer de esa misma información pero relacionada con nuestro pacientes, en el tiempo y lugar requerido, garantizándole la debida calidad en el tratamiento de sus datos y la eficaz seguridad de los mismos y más si tenemos en cuenta que estaremos utilizando la nube. Prácticamente utilizamos, aunque sin darnos cuenta, ciertas formas de cloud computing como por ejemplo Facebook, MySpace, etc. y cuentas de correo electrónico basadas en web como Gmail, así que estamos utilizando la nube. El cloud computing nos proporciona una infraestructura eventualmente ilimitada para almacenar y ejecutar datos y programas de pacientes, no necesitando tener infraestructura propia, sino acceso a la web.

» Propuestas de líneas de investigación.

En el mundo sanitario, esto supone una gran ventaja de cara a la actual globalización del paciente, ya que la información del mismo estará a su disposición en cualquier centro sanitario o lugar en que se la necesite, y solo con el consentimiento del mismo. No requiere de una gran inversión inicial tan desmesurada como hasta ahora y únicamente se pagara por los servicios y recursos que se vayan a necesitar. Cabe por ejemplo, para entender su importancia, que nos encontremos actualmente en Japón y que se requiera de nuestra historia clínica para poder tratarnos de alguna afección; con un solo punto que encontráramos de acceso a la web, y una vez identificados, en cuestión de segundos dispondríamos de ella, etc.

Potenciar la investigación en la seguridad de los datos del paciente es mejorar la seguridad y la calidad en la atención al paciente. Seguridad que nos da el cloud computing. Este es el presente y su permanente mejora será el futuro. La realidad que estamos viviendo la hacen necesaria.