Sociedad Española de Informática y Salud · Nº 104 · Abril 2014

I+S

INFORMATICA Y SALUD

ESPECIAL
Seguridad y Protección de Datos de Salud

XI Foro de Seguridad y Protección de Datos de Salud

III Reunión de la Red de Responsables de Seguridad de la Información Sanitaria

Entrega de los Premios SEIS 2013

Foros y Sectores

Entidades Asociadas

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

accenture
Alto rendimiento. Hecho realidad.

Ibermática
Tecnología y Conocimiento

BULL

INTERSYSTEMS

Bilbomática

ORION HEALTH

Carestream

SAVAC Consultores
MEDICAL APPLICATIONS SUPPORT

Tecnocom

CSC

T-Systems

ERESA
GRUPO MÉDICO

sistemas genómicos
servicios de análisis genético

VIDAL VADEMECUM INTERNACIONAL
A VIDAL GROUP COMPANY

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Director
Salvador Arribas

Comité editorial
Luciano Sáez
Marcial García Rojo
Rosa Valenzuela
Elvira Alonso
José Luis Carrasco

Consejo de Redacción
Rodrigo García Azurmendi
Miguel Chavarría
Fernando Bezares
José Quintela
Alberto Gómez Lafón
Jesús Galván
María Rovira
Julio Moreno
José Luis Monteagudo
Cristina Cuevas
Begoña Otalora
Emilio Aced
Fernando Escolar
Carlos García Codina
Vicente Hernandez
Carlos Hernández
Juan Fernando Muñoz
Juan Manuel de León
Carlos Parra
Antonio Poncel
Francisco Javier Francisco Verdú
Carlos Royo
José Lagarto
Isabel Aponte
Guillermo Vázquez
Javier Carnicero

Colaborador Técnico
Diego Sáez

Información, Publicidad, Suscripciones y DISTRIBUCIÓN:
CEFIC. C/ Enrique Larreta, 5 Bajo Izda
28036 Madrid
Tlfno: 913 889 478 • Fax: 913 889 479
e-mail: cefic@cefic.es

Producción Editorial:
Tel. 902 271 902 • 987 27 27 27
E-mail: mic@editorialmic.com
www.editorialmic.com
Editorial MIC

DL: M-12746-1992
ISSN: 1579-8070

Año 2014. Sumario nº 104

Editorial 5

ESPECIAL: Seguridad y Protección de Datos de Salud
- La Generación de Confianza en los Nuevos Entornos de Tratamientos de Datos de Salud 7
- El Principio de Limitación de la Finalidad a Debate: los Usos Secundarios 9
- Algunas Reflexiones sobre la Interacción entre Sanidad y Protección de Datos Personales 11
- Seguridad mhealth: Caso Práctico 13
- Experiencia TELBIL de Telemonitorización de Pacientes Complejos Manejo de la Confidencialidad 15
- Las TIC en Osakidetza. Cómo dar respuesta a nuestros pacientes del siglo XXI 17
- La experiencia de las autoridades de protección de datos. Casos Prácticos 19
- Datos Personales de Salud y Dispositivos Móviles: "mHealth" 21
- La Tormenta (im)perfecta 23
- Situación de la Movilidad en Cataluña 25
- Mensajería Instantánea para Uso Clínico 27
- La práctica de la medicina en tiempos de multimorbilidad y Big Data 29
- Ippok Comunidad Sanitaria, nuevo entorno de intercambio de información en salud 30
- En Busca de una Industria más Competitiva a través de la Investigación Europea en Seguridad TIC 32

ACTIVIDADES DE LA SEIS
- Entrega de los Premios SEIS 2013 34
- XI Foro de Seguridad y Protección de Datos de Salud 40
- III Reunión de la Red de Responsables de Seguridad de la Información Sanitaria 55
- IV Reunión del Foro de Interoperabilidad en Salud 59
- XI Congreso Nacional de Informática y Farmacia 2014 61
- XXI Jornadas Nacionales de Informática Sanitaria en Andalucía 63

Foros
- Foro de Seguridad y Protección de Datos 64
- Foro de Interoperabilidad 66
- Foro de Telemedicina 67

Noticias por sectores
- Medicina 71
- Farmacia 72

Agenda SEIS 2014 75

COLABORADORES TECNOLÓGICOS

AGFA HealthCare · CSC · Informática El Corte Inglés · InterSystems · EMC² · intel · gmv · T-Systems · Atos · FUJITSU · Microsoft

Los artículos revisiones y cartas publicadas en I+S, representan la opinión de los autores y no reflejan la de la Sociedad Española de Informática de la Salud

Entidades Colaboradoras

AGENCIA CATALANA DE PROTECCIÓN DE DATOS

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

EVERIS

OSAKIDETZA - SERVICIO VASCO DE SALUD

ABELLO LINDE

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ

IDCSALUD

MUTUA UNIVERSAL

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

COMPLEJO HOSPITALARIO UNIVERSITARIO DE SANTIAGO DE COMPOSTELA

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

VALLPLASA ATENCIO PRIMARIA

La Seguridad de la Informacion de Salud

A través de las actividades de la Sociedad Española de Informática de la Salud (SEIS) detectamos problemas o acciones que es necesario abordar en el sector sanitario con el fin de que la implantación de proyectos de innovación mediante las TIC se realice con las debidas garantías de funcionamiento y en las condiciones adecuadas, tanto desde el punto de vista tecnológico, como en su relación con los profesionales o los pacientes.

Por ello, un tema en el que la Sociedad Española de Informática de la Salud lleva trabajando desde hace muchos años es la promoción de medidas que garanticen la Seguridad y la Protección de Datos de Salud. Este tema lo consideramos vital para la extensión de proyectos TIC en nuestro sistema de salud, ya que, además de cumplir una garantía establecida en la ley, sobre el derecho de los ciudadanos a la protección de sus datos de salud, es imprescindible, por la dependencia cada vez mayor de las organizaciones de sus herramientas tecnológicas, que exigen la disponibilidad permanente de los servicios y la garantía de la custodia y recuperación total de la información.

En 2013, modificamos el nombre del Foro de Protección de Datos de Salud incluyendo la palabra Seguridad. Este hecho, junto con la creación de un grupo de trabajo denominado "Red de Responsables de la Seguridad de la Informacion de Salud", obedece a la demanda que nos llegaba a través de los profesionales responsables de la seguridad en los servicios y centros sanitarios de la necesidad de compartir experiencias y esfuerzos en este ámbito. Además, gracias al estudio que estábamos realizando sobre las TIC en el sistema sanitario (ÍNDICE SEIS) detectamos que, en el apartado de seguridad, había una situación alarmante en cuanto a dotación de recursos, tanto tecnológicos como humanos y, lo que es más preocupante, que existían importantes problemas organizativos.

Este grupo "Red de Responsables de Seguridad de la Informacion de Salud" inicia sus trabajos en marzo de 2013, con el principio base de compartir el conocimiento de los problemas a los que se enfrentan los departamentos de seguridad de la información sanitaria y las soluciones encontradas y, además, proponer aquellas medidas que se consideren necesarias para garantizar la seguridad de los sistemas de información.

La Sociedad Española de Informática de la Salud va a poner todos los medios a su alcance para que los trabajos y recomendaciones resultantes de este nuevo Comité Técnico de la SEIS tengan el alcance necesario para su traslación al sector sanitario.

Especial

Seguridad y Protección de Datos

INTRODUCCIÓN

La Sociedad Española de Informática de la Salud (SEIS) ha estado comprometida, desde los primeros momentos en que la protección de datos personales inició su andadura en España, con la promoción de este derecho en todos los ámbitos sanitarios y en la concienciación de los profesionales de la salud en la importancia de aplicar sus principios y en la necesidad y la obligación de respetar los derechos que a los ciudadanos otorga la legislación en esta materia.



Emilio Aced

Para ello siempre ha contado con la ayuda y el apoyo generoso de las autoridades de protección de datos de nuestro país, la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y, hasta su supresión, de la Agencia de Protección de Datos de la Comunidad de Madrid. Esta ayuda y apoyo se siguen manifestando año tras año en multitud de ocasiones y, especialmente, en la decisiva contribución de las mismas al éxito de las ediciones del Foro de Seguridad y Protección de Datos de Salud, que este año ha alcanzado su decimoprimera edición.

Además, este año se conmemora el X aniversario del establecimiento de la Agencia Vasca de Protección de Datos y, por este motivo, desde este número especial dedicado a la protección de datos personales, la SEIS quiere enviarle a su Director y a todos los profesionales que en ella trabajan y han trabajado desde su fundación, nuestra afectuosa felicitación por la gran labor que han realizado a lo largo de estos diez años y nuestros mejores deseos para el futuro de la institución.

Este número especial que tienen en sus manos –o en la pantalla de sus ordenadores o dispositivos móviles– se edita con motivo de la reciente celebración del XI Foro de Seguridad y Protección de Datos de Salud que se celebró en Pamplona los pasados días 19 y 20 de febrero y que, un año más, se constituyó en la cita de referencia para todos los interesados en la protección de datos y la privacidad en el sector de la salud.

En las páginas que siguen hemos invitado a los participantes en el Foro a compartir sus experiencias con los lectores de I+S en el ámbito del tema que fue el hilo conductor del Foro: Salud 2.0 y los entornos de movilidad conocidos como mHealth o mSalud. Estos dos ámbitos son más importantes cada día que pasa y encierran grandes promesas (y, en muchos casos, ya realidades constatables) para la mejora de la atención sanitaria a los pacientes, el apoyo permanente a los mismos, la comunicación entre los profesionales sanitarios y la optimización de la prestación y la gestión de los servicios sanitarios. En cualquier caso, uno de los retos más importantes en el despliegue de estos nuevos modelos de gestión y atención sanitaria es su implantación de tal manera que se aprovechen todas sus ventajas y potencialidades al mismo tiempo que se respetan los derechos y libertades de aquellos cuyos datos se tratan en estas nuevas plataformas.

El XI Foro de Seguridad y Protección de Datos se ocupó, pues, fundamentalmente, de la búsqueda de este equilibrio y de la presentación de casos de éxito en los que se habían conjugado satisfactoriamente ambos aspectos; incluyendo la confidencialidad y seguridad de la información en la atención domiciliaria a los enfermos crónicos, los riesgos específicos de la utilización de los dispositivos y aplicaciones móviles en el ámbito sanitario y las situaciones y la problemática que se produce cuando se utilizan los nuevos entornos de intercambio de información de salud como blogs, redes sociales o grupos de profesionales o de apoyo a pacientes con finalidades asistenciales o para compartir experiencias y proporcionar servicios sanitarios personalizados.

Del mismo modo, en estas páginas también podrán encontrar cumplida información sobre una de las más recientes iniciativas de la SEIS: el Comité Técnico de Seguridad de la Información Sanitaria (que comenzó su andadura hace apenas un año como Red de Responsables de Seguridad de la Información Sanitaria). En la reseña preparada por nuestro compañero Juan Díaz, Coordinador de dicho Comité, se informa de los objeticos de dicho Comité, de sus miembros, de los medios de que dispone y de los proyectos realizados y de los que se pondrán en marcha en breve.

Espero que este número especial sobre protección de datos personales les resulte interesante y que puedan extraer de él información y experiencias que les ayuden a implantar en sus organizaciones políticas de seguridad y privacidad robustas y fiables; particularmente, si han comenzado ya o están pensando en llevar a cabo experiencias interactivas que impliquen a pacientes y profesionales sanitarios y proyectos de movilidad y atención domiciliaria a enfermos crónicos.

La Generación de Confianza en los Nuevos Entornos de Tratamientos de Datos de Salud



José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos siempre ha prestado una atención especial a los tratamientos de datos personales que se producen en el ámbito sanitario por dos motivos esenciales. El primero de ellos es el carácter especialmente protegido y sensible de los datos de salud y las graves consecuencias que se pueden derivar para las personas de un uso negligente de los mismos, derivado del incumplimiento de las normas establecidas en la legislación de protección de datos. Estas consecuencias existen tanto desde el punto de vista de las implicaciones para la salud como en relación al acceso por terceros no autorizados, ya sean internos o externos a la organización responsable.

El segundo aspecto es su carácter universal ya que afectan a la totalidad de la población. En efecto, desde que nacemos se nos abre una historia clínica y los datos relativos a nuestra salud comienzan a ser recogidos, archivados y analizados con el fin de proporcionarnos una atención sanitaria eficiente y de calidad, no solo en los centros sanitarios sino también en entornos domésticos y en movilidad.

Por ello, la integridad, la confidencialidad y la seguridad de los datos de salud deben ser objetivos irrenunciables del sistema sanitario y, en particular, como se ha puesto de manifiesto en el XI Foro de Seguridad y Protección de Datos recientemente celebrado en Pamplona, cuando cada vez más los datos de salud abandonan los centros sanitarios y comienzan a ser tratados desde el domicilio de los pacientes crónicos o por proveedores de servicios de cloud computing y en multitud de dispositivos móviles y, a través de ellos, se comparten con otros profesionales o con otros pacientes con enfermedades similares a través de blogs, redes sociales o grupos de apoyo a pacientes.

Estas nuevas formas de tratamiento y acceso a la información proporcionan a los pacientes enormes oportunidades y ventajas -que solo están comenzando a ser exploradas- para mejorar sus tratamientos y, también, en la comunicación entre profesionales y entre profesionales y pacientes. Para que estas oportunidades puedan desarrollar todo su potencial es necesario –es más, es un factor crítico y esencial para su despliegue- generar la debida confianza en que todo se llevará a cabo con el más estricto respeto a los derechos de los pacientes y con las garantías adecuadas de que la información sanitaria será correcta e íntegra y estará disponible en todo momento en el lugar en que se la necesite pero que solo será accesible a quien esté autorizado a ello sin que nadie más pueda interferir y obtener un acceso ilícito a la misma.

La generación de confianza entre los afectados es un proceso sistemático y continuado que debe basarse en la transparencia respecto de los tratamientos de datos personales que se llevan a cabo, en la certeza de que se han tenido en cuenta todos los riesgos a que dichos datos personales están o pueden estar sometidos y en que se han tomado las medidas adecuadas para eliminarlos o mitigarlos en la medida de lo posible.

Para ayudar en este empeño, la Agencia Española de Protección de Datos acaba de presentar en su Sexta Sesión Anual Abierta un borrador de una "Guía para una Evaluación de Impacto en la Protección de Datos Personales" (EIPD), que tiene como objetivo, precisamente, esta necesaria generación de confianza, ofreciendo a todas las organizaciones y, en particular, a las del sector sanitario, una herramienta que les ayude a identificar, de una forma proactiva y en las primeras fases del desarrollo de nuevos productos, servicios y sistemas de información, los riesgos que dichos tratamientos tienen para la privacidad de las personas y a adoptar las medidas necesarias para eliminarlos o mitigarlos antes de que se materialicen.

Estas EIPD forman parte y son una herramienta im-

prescindible de lo que se conoce como Privacidad o Protección de Datos desde el Diseño, aproximación que persigue que todos los aspectos relativos a la privacidad y a la protección de datos personales estén presentes y se tengan en cuenta ya desde las fases iniciales de desarrollo de los nuevos productos y servicios y, de esta manera, se garantice el debido respeto a la privacidad de los titulares cuyos datos son procesados.

La gran ventaja derivada de la realización de una EIPD en las etapas iniciales del diseño es que permite identificar los posibles riesgos y corregirlos anticipadamente, evitando los costes derivados de descubrirlos a posteriori, cuando el producto, servicio o sistema de información está en funcionamiento o, lo que es peor, cuando la lesión de los derechos de los ciudadanos ya se ha producido.

En estos casos no sólo se incurre en costes económicos, sino también de imagen para la organización cuya reputación se ve afectada. Y, lo que es más importante, se han podido producir perjuicios o daños irreparables a personas que confiaron en una determinada organización sanitaria y que han visto defraudadas sus expectativas de privacidad. Esta confianza es muy difícil de restaurar una vez perdida.

"La Guía pretende promover la cultura proactiva de la privacidad, proporcionando un marco de referencia para el ejercicio de ese compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas"

En España en estos momentos no existe una obligación legal de realizar Evaluaciones de Impacto de esta naturaleza en ningún sector o ámbito específico, aunque podría existir en breve si se aprueba el Reglamento europeo en los términos de la Propuesta de la Comisión Europea. En cualquier caso, si hay un sector en el que se deberían de introducir, por todas las razones apuntadas al inicio de este artículo, las EIPD es, precisamente, el sector sanitario.

Pero, en todo caso, con independencia de que exista o no una exigencia normativa, la AEPD considera que las Evaluaciones de Impacto en la Protección de Datos son una metodología que ha alcanzado ya un grado de desarrollo suficiente como para considerarla madura y plenamente incorporable a nuestro país. Su empleo mejorará las políticas y las prácticas de protección de datos en aquellas organizaciones que las lleven a cabo y ello va a contribuir, sin duda, a generar más confianza en los usuarios o clientes de las mismas.

La Guía pretende promover la cultura proactiva de la privacidad, proporcionando un marco de referencia para el ejercicio de ese compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas. Además, está concebida como un marco flexible, que proporcione un modelo estructurado en el que apoyarse a la hora de realizar las Evaluaciones de Impacto, pero que no es invariable, sino que, mientras se respeten sus aspectos fundamentales, cada organización podrá (e incluso deberá) adaptarlo a su estructura, a su cultura y a sus necesidades.

Por lo tanto, además del marco de referencia que configure la Guía, la Agencia siempre dará la bienvenida a iniciativas procedentes del sector sanitario que, manteniendo los elementos esenciales contenidos en ella, propongan las modulaciones o especificaciones que sean convenientes para adaptar esos elementos esenciales a las características específicas de este sector tan complejo y crucial en nuestra sociedad.

No obstante, el documento que ha presentado la AEPD no es la versión definitiva de la Guía sino un borrador, ya que queremos contar con la opinión de todos los interesados para elaborar el documento final de forma participativa. Por ello, se ha abierto un periodo de consulta pública hasta el 25 de abril de 2014. Durante este tiempo el borrador de la Guía y el cuestionario de la consulta estarán disponibles en la web de la Agencia (www.agpd.es). Aprovecho esta ocasión para animar a todos los lectores de I+S a participar en la misma y a enriquecerla con sus observaciones y propuestas.

Finalmente, les adelanto que cuando se publique la versión definitiva, la realización de una Evaluación de Impacto siguiendo las directrices de la Guía, aunque no podrá ser considerada como un criterio de exención de eventuales responsabilidades en caso de que se incurra en vulneración de la normativa de protección de datos, sí va a ser tenida en cuenta por la Agencia como un elemento relevante a la hora de valorar si se ha adoptado la diligencia debida en la implementación de las medidas adecuadas para cumplir con las exigencias legales.

El Principio de Limitación de la Finalidad a Debate: los Usos Secundarios



María Ángels Barbarà i Fondevila
Directora. Autoridad Catalana de Ptotección de Datos

Pese a que el debate en torno al principio de finalidad no es nuevo, los nuevos avances tecnológicos, como el *Big Data*, el *cloud computing* o el *Internet of Things* lo han hecho resurgir con fuerza. Los datos se han convertido en un activo muy apetecible para empresas y gobiernos, especialmente desde una nueva perspectiva, la de los usos secundarios de la información; usos que, en el momento de la recogida de los datos, pueden ser no conocidos. Por tanto, nuevas posibilidades reabren viejos debates con una nueva dimensión.

La configuración del derecho a la protección de datos o derecho a la autodeterminación informativa, a partir del control que la persona puede ejercer sobre su propia información, adquiere en la actualidad una nueva virtualidad, que hace necesario un replanteamiento de cuestiones como el alcance de los principios de finalidad, consentimiento e información.

Es innegable que la posibilidad de control sólo puede ser efectiva si el titular de la información (el interesado) tiene los instrumentos necesarios para ejercerlo.

Los elementos primarios para ejercer este control están consagrados por tres principios esenciales: principio de limitación de la finalidad, principio de información y principio de consentimiento. Todos ellos vinculados y todos ellos centrados en el conocimiento exacto de qué, quién y cómo se utiliza la información personal. Sin conocimiento, no puede existir protección.

El propio concepto de autodeterminación informativa conlleva que el interesado debe asumir un elevado grado de responsabilidad respecto a su información. Ello no significa que tenga toda la responsabilidad (todo aquel que interviene en un tratamiento de datos personales asume, en mayor o menor medida, cierto grado de responsabilidad), pero sí una parte importante de ella. En definitiva, la posibilidad de decidir sobre la propia información a partir de principios como el del consentimiento y la información es clave en la asunción de esa responsabilidad.

Si hasta el momento parecía que los principios antes indicados eran internacionalmente aceptados como parte indisoluble del derecho a la protección de datos, ahora, ante la nueva realidad tecnológica, surgen opiniones que consideran que estos principios deben ser limitados, es decir que no debe trasladarse al interesado la responsabilidad sobre los tratamientos de datos realizados por terceros.

Alrededor de esta cuestión ha surgido un interesante debate, a raíz de la publicación del documento *Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines*[1] y de los comentarios vertidos por Viktor Mayer-Schönberger, respecto a la necesidad de limitar los principios de información y consentimiento atendiendo a su poca efectividad en la práctica y vistas las posibilidades de usos secundarios que permiten los nuevos avances tecnológicos. En la propuesta de revisión de las Directrices de la OCDE de 1980, los autores manifiestan que se ha hecho un esfuerzo deliberado para desviar el foco de atención de los mencionados principios. Consideran que en la actualidad, tal y como están planteados, han dejado de ser efectivos, y que, por ejemplo, la mayoría de las personas no lee las políticas de privacidad que acepta. Incluso si quisieran hacerlo les resultaría imposible, ya que, según un estudio del año 2008, para leer las políticas de privacidad de sólo algunos de los sitios web más populares serían necesarias unas 244 horas. A esto hay que añadirle la dificultad de lectura y la imposibilidad de elegir ante la "necesidad" de utilizar los servicios que se

1. *Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines, december 2013.*

quieren obtener. Por descontado, también, los nuevos avances tecnológicos como el Big Data, que reconvierten la información en nueva información para nuevas finalidades no previstas en el momento de la recogida de los datos.

Ante este planteamiento, el pasado 5 de marzo se publicó *The Unintended Consequences of Privacy Paternalism*[2]. En este caso, los autores consideran que la propuesta de revisión de los principios de la OCDE supone una aproximación paternalista a la protección de datos que sólo puede conllevar una disminución de la privacidad en el siglo XXI. Pese a ser conscientes de la realidad de las actuales políticas de privacidad, consideran que las personas continúan teniendo expectativas respecto a cómo serán utilizados sus datos, atendiendo al motivo y a la finalidad de su recogida, y que limitar estos principios dejando fuera al titular de los datos lo hace vulnerable frente a las decisiones adoptadas por otros.

"La anonimización de la información tiene un papel preferente en el entorno sanitario. Pero debemos recordar que hay que extremar las medidas para evitar, en un sector tan sensible como el sanitario, que los instrumentos adoptados para ello sufran fugas en el transcurso de la ejecución del proyecto"

En todo este debate, es importante tener en cuenta que son las nuevas técnicas de recogida, análisis y conservación de datos las que hacen necesario un replanteamiento de los principios de protección de datos. La importancia de la información, su valor como activo, se ha trasladado de los usos primarios de la información (aquellos que motivaron la recogida de la información en el inicio del proceso) a los usos secundarios (aquellos que, probablemente, no eran ni conocidos ni esperados en el momento de la recogida de la información). Los enormes beneficios, en todos los contextos, que pueden generar estos usos secundarios de la información deben ser compatibilizados con la garantía de los principios esenciales de la autodeterminación informativa, donde consentimiento e información son pilares esenciales del derecho. No podemos utilizar instrumentos de garantía de defensa si no sabemos de qué debemos defendernos.

Los usos secundarios son especialmente relevantes en el ámbito de la salud, donde tienen una importante virtualidad para la mejora de la calidad de los servicios, en la investigación médica, en la planificación y administración sanitaria y en salud pública, entre otras muchas posibilidades. Pero, como hemos visto, los usos secundarios incrementan los riesgos para la privacidad. El "contexto", que hasta ahora venía delimitado por el momento de la recogida, se diluye ante la magnitud de las posibilidades generadas por las nuevas tecnologías de análisis de datos. Ante esto la anonimización, que ha sido utilizada tradicionalmente para generar valor protegiendo la privacidad, puede convertirse, en el cambio de paradigma que estamos viviendo, en una nueva forma de gestión de la información en un momento en el cual los usos inciden directamente en las personas.

En Cataluña, en junio de 2013 se aprobó por Acuerdo de Gobierno poner en marcha el Proyecto VISC+[3] (Más Valor en la Información de Salud en Cataluña) que, en el contexto del open data, pretende favorecer la transparencia y la generación de valor a partir del acceso a la información, en este caso en el sector sanitario. Este proyecto se basa en el tratamiento de información anónima para generar conocimiento a partir de esta información. Se configura como un proyecto de colaboración público-privada, para diseñar un nuevo modelo de gestión, explotación y análisis que permita dar más valor a la información generada en el sistema sanitario.

Así, la anonimización de la información tiene un papel preferente en el entorno sanitario. Pero debemos recordar que hay que extremar las medidas para evitar, en un sector tan sensible como el sanitario, que los instrumentos adoptados para ello sufran fugas en el transcurso de la ejecución del proyecto. La privacidad en el diseño vuelve a ser un elemento clave para el correcto desarrollo de un proyecto que permitirá generar un enorme valor para la sociedad, al mismo tiempo que se garantiza la privacidad y se mantiene y refuerza la confianza de los ciudadanos.

En definitiva, el enfoque político, los modelos de negocio, las normas sociales y la tecnología han variado en los últimos años, se han transformado, y el análisis de la información se ha convertido en el nuevo motor para la creación de valor económico y social.

2. The Unintended Consequences of Privacy Paternalism. Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada Khaled El Emam, Ph.D. Canada Research Chair in Electronic Health Information University.

3. http://www20.gencat.cat/portal/site/canalsalut

Algunas Reflexiones sobre la Interacción entre Sanidad y Protección de Datos Personales



Iñaki Pariente de Prada
Director de la Agencia Vasca de Protección de Datos

Hay algunas cuestiones que pueden tener una gran incidencia en el futuro en el sector sanitario, y que entran desde luego dentro de lo que podríamos denominar una estrategia en materia de protección de datos en el ámbito sanitario de las agencias de protección de datos.

En cuanto a los datos que afectan directamente al sector de los datos de salud, creo que podemos hablar de dos tipos de cuestiones, o que podríamos distinguir las cuestiones en dos partes. En primer lugar, las cuestiones que vienen siendo tradicionalmente interesantes para el sector, que son recurrentes, pero no han sido resueltas aún. Pero por otro lado, algunas cuestiones nuevas que están surgiendo en los últimos tiempos y que en el futuro serán de gran interés, sobre todo las relativas a las nuevas tecnologías. En particular, aquellas relativas a la e-medicina, o las aplicaciones móviles y las redes sociales y su papel en el desarrollo de la sanidad.

El primer tipo serían las cuestiones que llamaré "recurrentes", que siguen planteando problemas y lo seguirán haciendo en el futuro sin duda alguna, aunque en algún caso con nuevos matices, como la aplicación del derecho de cancelación en el ámbito sanitario, a la luz de la nueva regulación que surja en el Reglamento Europeo del derecho al olvido o a la supresión de datos. Asimismo, todo lo relativo a los derechos ARCO y su aplicación en el ámbito sanitario, son elementos recurrentes, pero con nuevos matices, debido a la entrada de elementos tecnológicos y del uso de internet. Por ejemplo, la regulación del derecho de acceso mediante medios electrónicos, el acceso a la historia clínica del paciente mediante tarjetas o claves de seguridad, la posibilidad del paciente de "escribir" en la historia clínica o manifestar opiniones o datos de todo tipo, etc.

Estos derechos plantean evidentes problemas de aplicación práctica: A modo de ejemplo:

¿puede un ciudadano acceder a su historia clínica y solicitar el derecho de rectificación en relación con un dato que consta en el expediente y con el que no está de acuerdo?

¿puede un ciudadano solicitar que un determinado dato que consta en el expediente sea cancelado?

¿puede plantear una oposición a un dato concreto?

Una evolución posterior de los derechos ARCO es la aparición en escena del derecho al olvido con el proyecto de Reglamento Europeo de protección de datos, del que francamente tengo dificultad para prever qué implicaciones tendrá en el ámbito de los datos de salud, o de las instituciones sanitarias.

En todo este sector, las agencias de control han desarrollado una amplia doctrina y se sigue haciendo en el presente. Sin embargo, todo indica que seguirá siendo un sector conflictivo, como hemos podido apreciar en nuestra actividad como institución de control, al intentar tratar con la Administración sanitaria cuestiones como la confidencialización, la oposición al tratamiento, la cancelación, etc. y su puesta en práctica.

Otras cuestiones recurrentes y clásicas en este ámbito son el establecimiento de medidas de seguridad en el acceso a los expedientes, medidas que en buena parte tienen un componente organizativo, que se revelan en muchos casos sencillas: deber de secreto y confidencialidad de los datos, fijación de obligaciones claras en el documento de seguridad, formación del personal sanitario y administrativo en las obligaciones básicas de protección de datos personales, etc.

Pero sin embargo, y a pesar de este evidente gran sector de problemas que tradicionalmente viene apareciendo en el ámbito de la relación entre protección de datos y sector sanitario, también hay algunas otras cuestiones que van llegando de la mano sobre todo de los avances tecnológicos.

Entre estos se encuentra todo lo relativo a E-sanidad, el acceso de los pacientes/ciudadanos a su expediente médico, la elaboración de un historial médico único de toda la Administración sanitaria

en su conjunto, para conseguir un tratamiento global del paciente, el uso del cloud computing en el ámbito sanitario, o la telemedicina, la vigilancia y seguimiento de pacientes crónicos en el domicilio, u otros.

En relación con la E-sanidad, es importante conocer en primer lugar los datos sobre posición de los ciudadanos, recabados en una encuesta realizada por el Observatorio Nacional de las Telecomunicaciones titulada "Los ciudadanos ante la e-Sanidad", por su gran relevancia, y de los que recogemos algunos a continuación.

"Destaca muy positivamente el conocimiento que tiene la población española de las herramientas más importantes de la e-sanidad, como son la Historia Clínica Electrónica (78,2%), la petición de cita médica a través de Internet (64,8%) y la receta electrónica (56,2%)"

En cuanto al uso de Internet como fuente de información y proveedor de servicios sanitarios: ¿Por quién y para qué se utiliza Internet en términos de información sobre salud? Son las mujeres (54%), personas entre 25 y 49 años (51%) y que viven en núcleos urbanos (49,8%) los que más utilizan Internet para temas relacionados con la salud. Además, resulta destacable que cerca del 30% de la población internauta se ha dirigido a Internet para consultar temas sanitarios en la última semana, mientras que el 36,2% lo ha hecho en el último mes. Se accede mayoritariamente a webs privadas (59%) y en menor medida a webs de instituciones públicas (41,4%) hay más confianza en estas últimas. La obtención de información sobre enfermedades se convierte en el tema u objetivo de información más recurrente (40%), ya sea para conocer sobre una enfermedad, su tratamiento o prevención, etc. El 35% de los internautas realiza la petición de cita médica a través de la red. En menor medida se utiliza Internet para citas con especialistas (11%), modificaciones en la Tarjeta Sanitaria (5,2%) u otras acciones administrativas – por ejemplo cambio de médico – (5,1%).

En cuanto al uso de redes sociales como fuente de información para temas de salud un 12,8% de los internautas (3,8% de la población), utiliza las mismas, aunque se señala que la confianza en estas es mínima.

Actualmente es Wikipedia la red social más utilizada por estos pacientes (72%), Facebook es utilizada por 35,1%, y en menor medida se situarían Youtube 30,8%) y Twitter (13,3%). Aún con un nivel de confianza bastante bajo, con las redes sociales se busca aclarar dudas (38,9%), y conocer y compartir experiencias de salud similares con otras personas (26,1%).

En cuanto a la e-sanidad, destaca muy positivamente el conocimiento que tiene la población española de las herramientas más importantes de la e-sanidad, como son la Historia Clínica Electrónica (78,2%), la petición de cita médica a través de Internet (64,8%) y la receta electrónica (56,2%).

En general, todas estas herramientas son percibidas con un alto grado de utilidad (superior a 8/10 puntos) por parte de los ciudadanos, lo cual muestra un interés importante en su posible uso futuro.

Además el paciente apoyaría la idea de que el médico tenga un blog o Web con información y consejos de salud (71,9%). Son sobre todo los perfiles más jóvenes y la gente con una mejor valoración de su estado de salud autopercibido quienes se muestran más dispuestos a participar en este tipo de iniciativas.

A modo de conclusión, las nuevas tecnologías están influyendo de manera positiva en la gestión, implantación e información que, sobre temas relacionados con la salud, llega al ciudadano. Hay camino por recorrer, fundamentalmente en la implantación efectiva de diversas aplicaciones y herramientas destinadas a ayudar a mejorar la calidad de vida de los pacientes de manera general y de forma particular a mejorar el tratamiento de algunas enfermedades, pero el primer paso en algunos casos está dado: son elementos ya conocidos por los ciudadanos y, lo que es más importante, son igualmente reconocidos y valorados por su utilidad para la gestión de su salud. Si nos fijamos en el ámbito de la información, Internet puede convertirse en un elemento clave para hacer llegar al paciente información, datos, análisis que ayuden a comprender cómo es su estado de salud, identificar pautas de prevención o ayudarle a llevar de una manera más sosegada y objetiva su enfermedad.

Y una llamada de atención en todo este nuevo sector de problemas que surge para la protección de datos personales y la seguridad de los mismos, algo que debe estar presente en toda implantación de nuevos mecanismos y sistemas en el futuro.

Seguridad mhealth: Caso Práctico



Miren I Bagües y Gimena Rodríguez
Saludnova, www.saludnova.com, saludnova@saludnova.com

mHealth o salud móvil define las prácticas de salud que se realizan mediante dispositivos móviles que utilizan tecnologías inalámbricas para intercambiar información y conectar a los diferentes actores autorizados[1].

INTRODUCCION

La seguridad en el entorno de la mhealth es esencial y debe afrontar la gestión de la identidad de acuerdo a las últimas tendencias y normativas vigentes, de forma que los usuarios puedan acceder e intercambiar la información de forma segura garantizando en todo momento la confidencialidad e integridad de los datos consultados o almacenados en el terminal, aunque sean datos almacenados en el dispositivo con carácter temporal.

Según un estudio[2] el 97% de los usuarios de teléfonos inteligentes estáde acuerdo en que la privacidad es una de las principales preocupaciones pero pese a esta preocupación sólo el 52% de los usuarios han leído la política de privacidad de una aplicaciónmóvil.

Actualmente no existe una solución robusta, interoperable e independiente de la plataforma que permita la gestión de la identidad y la confidencialidad en los dispositivos móviles de los usuarios. Esto se debe a que hasta hace poco no se contemplaban los dispositivos móviles para escenarios con restricciones de confidencialidad y seguridad tan elevados como el sanitario. Lo que sí existe son recomendaciones y buenas prácticas que buscan, por un lado, que la seguridad y la privacidad sea una parte esencial y prioritaria del producto/servicio y por otro lado, el establecimiento de unos mínimos razonables dados por defecto para de esta manera liberar al usuario, el cual ignora la naturaleza de esta problemática. En este contexto, cobra peso una opción denominada el PrivacybyDesign, traducida como "la privacidad desde el diseño".

El principio de PrivacybyDesign significa que la protección de la intimidad y los datos personales se tienen en cuenta a lo largo de todo el ciclo de vida de las tecnologías, desde su concepción hasta su despliegue, utilización y eliminación final[3]. Esta opción contempla el desarrollo de escenarios de privacidad desde el diseño del negocio convirtiéndose de esta manera en una herramienta de producción positiva de resultados para la empresa, ya que la inversión en cumplimiento normativo posterior será mínima o tal vez innecesaria, gracias a que se tendrá en el mercado un producto o servicio, que se adecue a un estándar legal, con calidad y un excelente cumplimiento normativo, lo que les permitirá competir ofreciendo servicios adaptados a las necesidades del mercado.

Ana Cavouikian[4], la creadora canadiense de este principio, estableció 7 elementos importantes en la implementación del mismo:

1) Proactivo, no reactivo. Preventivo, no correctivo.
2) Privacidad como configuración predeterminada.
3) Privacidad incrustada en el diseño.
4) Funcionalidad total. Todos ganan, no si alguien gana otro pierde.
5) Seguridad extremo-a-extremo. Protección del ciclo de vida completo.
6) Visibilidad y transparencia. Mantenerlo abierto.
7) Respetopor la privacidad de los usuarios. Enfoque centrado en el usuario.

CASO PRÁCTICO: SALUDNOVA

Saludnova[5], es una empresa de mhealth, que proporciona soluciones ubicuas para las personas que requieren de forma puntual o periódica la monitorización de variables biométricas y/o la detección en tiempo real de situaciones de alarma, activando las medidas de atención necesarias, en busca de facilitar el mayor grado de bienestar a las personas.

Saludnovahace uso del principio de PrivacybyDesign en la conceptualización de sus soluciones. Para ello adapta continuamente su plataforma, y gracias a eso sus servicios, para incorporar los mecanismos necesarios para que los usuarios puedan cumplircon los mandatos relativos a la L.O.P.D vigente. Actualmente, algunos de los puntos más importantes

a tener en cuenta son: a) la correcta identificación y autentificación personalizada e inequívoca de usuarios, b) la limitación en el acceso a la información según permisos, c) la copia de respaldo y recuperación de los datos, d) el registro de acceso a la información y e) la protección de la información enviada a través de redes de comunicaciones. Concretamente a continuación vamos a enumerar alguno de los mecanismos adoptados en el diseño de la plataforma:

- Un primer mecanismo es la identificación de forma inequívoca de cada uno de los componentes hardware que intervienencon el fin de que únicamente aquellos componentes identificados puedan intercambiar información valida. Esto permite evitar posibles spam provenientes de fuentes externas.
- Para la identificación de los usuarios, y la limitación en el acceso, se ha decidido utilizar la identificación basada en usuario y contraseña segura asociada. Del mismo modo el usuario estará asociado bien a un dispositivo o bien a un rol concreto, describiendo de esta manera las funcionalidades a realizar dependiendo tanto del rol como de su identificación. En algunos casos concretos, también se soporta la identificación de software/hardware/usuarios a través de tecnologías criptográficas basadas en certificados digitales ampliamente utilizadas en otros dominioscomo el de la identificación ciudadana (DNIe) y la identificación del software (Izenpe).
- Para mantener la privacidad y seguridad en el sitio remoto, se utiliza el protocolo HTTPS, y para la transferencia de datos, el FTPS. También se incorpora una VPN entre los servidores y distintos periféricos, disponiendo de una red privada y segura.

BIBLIOGRAFÍA

[1] COCIR Glossary of terms.
[2] Lookout mobile security.www.truste.com.
[3] Una agenda digital para Europa. COM (2010) 245.
[4] Privacy by Design (Ann Cavoukian). Office of the Information and Privacy Commissioner. 2011.
[5] www.saludnova.com



Experiencia TELBIL de Telemonitorización de Pacientes Complejos
Manejo de la Confidencialidad



Dr. Iñaki Martín Lesende
Médico de familia. Centro de Salud San Ignacio, Bilbao

La experiencia TELBIL consiste en una experiencia de telemonitorización de pacientes con enfermedades crónicas desde la Atención Primaria (AP). Se realizó un ensayo clínico inicial (estudio TELBIL1, 2) y un posterior proyecto de implementación (proyecto TELBIL-A3), durante los años 2010-2014.

Las tres características principales de esta experiencia han sido:

- complejidad de los pacientes incluidos (pacientes domiciliarios o con mucha dificultad para salir de casa y acudir a los centros sanitarios, insuficiencia cardiaca y/o broncopatía crónica, 2 o más ingresos el año previo y al menos uno de ellos debido a estas patologías),
- protagonismo de la AP, donde son los médicos y enfermeras del Centro de Salud los principales encargados de la telemonitorización,
- riguroso desarrollo, evaluación y análisis de ambos proyectos.

La telemonitorización consistía en una transmisión diaria domiciliaria de ciertos parámetros clínicos según las características y patologías de los pacientes (frecuencia cardiaca/respiratoria, saturación de oxígeno, tensión arterial –TA-, peso, cuestionario de situación clínica respecto al día anterior); varios dispositivos, pulsioxímetro y tensiómetro, facilitados por bluetooth. Estos datos se transmitían, por GPRS desde un smartphone en el domicilio, a una plataforma web que es revisada por los profesionales, y que además está facilitada por un sistema de alertas cuando los valores sobrepasaban los datos establecidos en su situación basal.

Los resultados principales obtenidos han sido2, 4, 5:

- mayor porcentaje de pacientes sin ningún ingreso hospitalario al año de seguimiento,
- menor estancia hospitalaria durante los ingresos,
- incremento de contactos telefónicos y descenso de las visitas domiciliarias fundamentalmente de enfermería,
- mejor percepción de calidad de vida (CVRS) de los pacientes y menor sobrecarga de sus cuidadores,
- alto grado de satisfacción y aceptación con el proyecto, tanto de pacientes y sus familias y cuidadores, como de los profesionales sanitarios que participaban,
- sin incremento de gasto sanitario y con una tendencia a la disminución del mismo.

Un aspecto muy a tener en cuenta es que los pacientes transmitían sus datos clínicos hasta una plataforma web no integrada en la historia clínica ni en el circuito interno institucional. Por ello, las medidas que protegen la confidencialidad de los pacientes nos han parecido un aspecto básico desde el principio, y que siempre es necesario preservar. Aún a sabiendas que hoy añadiríamos otras, las principales medidas que adoptamos en ambos proyectos fueron:

1. Aprobación de los dos proyectos por el Comité de Ética (CEIC) y Comisiones de Investigación correspondientes. Pensamos que, en especial el primero, deben velar y asegurar el cumplimiento de las consideraciones que protejan al paciente y los aspectos éticos. Y debieran ser los primeros en orientar los proyectos en este sentido. Relacionado con ello está el recabar financiación para los proyectos a través de financiación externa y competitiva, donde vuelven a ser evaluados externamente en todos sus aspectos.
2. Codificación de los pacientes en todas las bases de datos, documentos y en la plataforma web. A los pacientes se les indicaba cuál era su código (TELBIL 1, TELBIL-A01, TELBIL-A30…), que era el que figuraba en los lugares donde se accedía y manejaban sus datos (plataforma web, bases de datos, acceso de otros profesionales encargados de su cuidado -por ej. "consejo sanitario", que forma parte de la atención no presencial del Servicio Vasco de Salud, Osakidetza-, etc.). La identificación de los pacientes solo estaba a disposición de los dos coordinadores de los proyectos, responsables de la empresa proveedora, y otros

profesionales concretos indicados.

3. Todos los pacientes (y profesional coordinador) firmaban un consentimiento informado duplicado, donde además de explicar el proyecto se les daba oportunidad de abandonarlo si así lo deseaban, se indicaba que sus datos tenían un tratamiento anónimo excepto ciertos profesionales, y también recogía alguna medida de seguridad en el sentido de actuar como lo hacían previamente, previendo situaciones de errores en la transmisión, recepción o interpretación de datos.



Paciente y cónyuge realizando la telemonitorización.

4. Restricción de acceso de los datos, mediante claves de diferente nivel de acceso, a las personas y profesionales directamente implicados. Un profesional solo podía acceder a los pacientes de su competencia, por ejemplo los de un Centro de Salud solo podían acceder a pacientes de ese centro y no al resto.
5. Medidas adoptadas por la empresa proveedora para cumplir la normativa en protección de datos y su seguridad y confidencialidad; aspecto que a su vez realizaban a través de los servicios de otra empresa especializada.

Con estas medidas tratábamos de asegurar este aspecto. Y nos satisface decir que los pacientes han confiado en esta confidencialidad. A la pregunta, en la reciente encuesta de satisfacción a pacientes y familiares que hemos realizado, de si "tenían confianza en que sus datos eran confidenciales y solamente los veía su médico o enfermera" han puntuado entre 1 a 5 con una media de 4.5, otorgando un 88% la máxima puntuación (5 sobre 5) y el 12% restante un 4 sobre 5.

BIBLIOGRAFÍA

1. **Martín-Lesende I, Orruño E, Cairo MC, Bilbao A, Asua J, Romo MI, et al.** Assessment of a primary care-based telemonitoring intervention for home care patients with heart failure and chronic lung disease. The TELBIL study. BMC Health Services Research 2011; 11:56. doi:10.1186/1472-6963-11-56
   Disponible en: http://www.biomedcentral.com/1472-6963/11/56#IDAOGQR1
2. **Martín-Lesende I, Orruño E, Bilbao A, Vergara I, Cairo MC, Bayón JC, et al.** Impact of telemonitoring home care patients with heart failure or chronic lung disease from primary care on healthcare resource use (the TELBIL study randomised controlled trial). BMC Health Services Research 2013, 13:118 doi:10.1186/1472-6963-13-118. Disponible en: http://www.biomedcentral.com/1472-6963/13/118/abstract
3. **Iñaki Martín Lesende.** Telemonitorización de pacientes crónicos pluripatológicos desde la Atención Primaria: experiencia TELBIL. Lecciones aprendidas. AMF 2013; 9 (11): 659-661
4. **Bayón JC, Martín-Lesende I, Cairo MC, Ortuño E, Asua J, Romo MI, et al.** Evaluación económica de una intervención de telemonitorización desde la atención primaria en pacientes domiciliarios con insuficiencia cardiaca y/o broncopatía crónica: Análisis coste-efectividad. Estudio TELBIL. Ministerio de Sanidad, Servicios Sociales e Igualdad. Agencia de Evaluación de Tecnologías Sanitarias del País Vasco; 2013. Informes de Evaluación de Tecnologías Sanitarias: OSTEBA Nº 2011/01.
   Disponible en: http://www9.euskadi.net/sanidad/osteba/datos/evaeco.insfca.bronc.pdf
5. **Martín-Lesende I, Orruño E, Bayón JC, Bilbao A, Vergara I, Cairo MC, et al.** Evaluación e impacto de una intervención de telemonitorización en pacientes domiciliarios con insuficiencia cardiaca y broncopatía crónica controlada desde la atención primaria. Ensayo clínico aleatorizado. Estudio TELBIL. Ministerio de Sanidad, Servicios Sociales e Igualdad. Agencia de Evaluación de Tecnologías Sanitarias del País Vasco; 2013. Informes de Evaluación de Tecnologías Sanitarias: OSTEBA Nº 2010/02.
   Disponible en: http://www1.euskadi.net/buscadorsan/osteba/infeva.apl y el pdf en http://www9.euskadi.net/sanidad/osteba/datos/eval_impactel.pdf

Las TIC en Osakidetza. Cómo dar respuesta a nuestros pacientes del siglo XXI



Mikel Ogueta Lana
Subdirector de Información Sanitaria y Calidad. Servicio Vasco de Salud. Osakidetza

En Osakidetza, en los últimos años, los Sistemas de información de Osakidetza han evolucionado actuando como motor en la transformación sanitaria necesaria para garantizar una atención adecuada a nuestra población.

Nuestros sistemas de información incluyen los puntos de vista de:

- Profesionales: Pasamos a un Sistema de información centrada en el paciente. Osabide Global. Historia electrónica única compartida por todos los profesionales, facilitando una completa Continuidad Asistencial.
- Pacientes: Participación activa de los pacientes a través de "Mi Carpeta de Salud", con la seguridad y accesibilidad mediante firma digital avanzada (identificador único, juego barcos, contraseña):
  - Pueden Ver información de todos informes y pruebas
  - Pueden añadir información por el propio paciente en Osabide Global:
    - Informes de centros ajenos a Osakidetza o privados.
    - Su diario (El paciente registra su información)
  - Pueden interactuar con el sistema sanitario a través de Carpeta:
    - Mensajes del médico al paciente.
    - Dudas con mi médico: posibilita consultas entre el médico y el paciente que se incorporan automáticamente en su historia clínica (sustituyendo el correo electrónico por un sistema seguro).

La transformación Sanitaria necesaria se fundamenta en 3 pilares:

1. Cambio Cultural: La persona como centro de nuestra atención, en lugar del profesional o el centro asistencial.
2. Cambios Organizativos:

Administrativos: OSIS Organizaciones de Servicios integrados Primaria-Especializada.

Cambios de roles de profesionales y pacientes adaptados a las necesidades.

3. Cambios en los Sistemas de información que faciliten e incorporen esta transformación (Osabide Global y Carpeta de Salud).

Las claves para facilitar el acceso y utilización de las TIC por nuestros profesionales y pacientes en la historia clínica las podemos resumir en 3S:

1. Seguridad: elemento imprescindible para un sistema de información sanitaria. La protección de datos es una garantía de seguridad tanto para los profesionales como para los pacientes. El gran reto es conseguir el equilibrio adecuado entre Seguridad y Accesibilidad, que facilite una atención eficiente diaria.
   Seguridad también es garantizar la accesibilidad a la información que evite errores médicos, optimice las decisiones clínicas y facilite la continuidad asistencial.
2. Sostenibilidad: Debemos hacer una atención sanitaria diferente adaptada a los tiempos actuales, que sea flexible según las necesidades. Incorporar la participación del paciente, además de aumentar su autonomía, también permite una utilización de los recursos sanitarios más adecuada.
3. Sencillez: Elemento clave (aunque muchas veces olvidado) para un uso generalizado y la incorporación de los pacientes como parte activa de su historia clínica. La sencillez para nuestros usuarios implica un esfuerzo funcional y tecnológico imprescindible.

Debemos proporcionar una atención óptima, centrada en los ciudadanos y sus cuidadores, en el momento oportuno en que lo necesite, gracias a la integración de la información, y considerar el domicilio del ciudadano, si es posible, el lugar idóneo para recibir los cuidados sanitarios que precise.

Los sistemas de información están facilitando una continuidad asistencial que en los últimos años ha posibilitado potenciar las alternativas a la hospitalización tradicional (incluyendo la telemonitorización), disminuyendo los ingresos hospitalarios de procesos médicos en los últimos 9 años en un 6%,

posibilitando un aumento en la actividad quirúrgica hospitalaria.
La atención sanitaria actual debe contemplar tanto la atención presencial clásica, como la atención no presencial, que posibilita recibir atención sin necesidad de desplazarse a los centros sanitarios. En este sentido Osakidetza la ha impulsado, con muy buena aceptación por la población, alcanzando el 20% de las consultas en atención primaria actualmente son consultas telefónicas solicitadas por el propio paciente.
Las consultas no presenciales son un complemento de la atención tradicional y están disponibles tanto para los profesionales como para los pacientes, con el fin de tener nuevas vías de comunicación entre pacientes y profesionales. De esta forma estamos aumentando la accesibilidad a nuestro sistema sanitario sin necesidad de duplicar servicios o de desplazamientos innecesarios.
Actualmente un paciente de Osakidetza ha aumentado su empoderamiento:

- Solicitar una consulta por Web.
- Acudir a una consulta presencial con acceso actualizado de todos sus evolutivos.

La Experiencia de las Autoridades de Protección de Datos. Casos Prácticos



Carles San José Amat
Jefe del Área de Inspección. Autoridad Catalana de Protección de Datos

A partir de un supuesto real denunciado ante la Autoridad Catalana de Protección de Datos (en adelante, APDCAT) me referiré al principio de calidad de los datos previsto en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), en su vertiente del principio de finalidad (artículo 4.2 de la LOPD) que viene a determinar que los datos personales no pueden utilizarse para una finalidad distinta o incompatible con aquellas para las que los datos hubieran sido recogidos.

El supuesto es el siguiente. Un empleado de un centro sanitario acudió a su puesto de trabajo en un centro de atención primaria (CAP) bajo los efectos del alcohol. En el transcurso de su jornada laboral se peleó con una persona usuaria. A raíz de esa pelea se solicitó la intervención de la Policía Local, cuyos agentes detuvieron al empleado y le trasladaron al Hospital con el fin de practicarle el pertinente reconocimiento médico. Este reconocimiento suele practicarse a las personas detenidas con la finalidad de evitar eventuales acusaciones de los detenidos en relación al trato recibido por las fuerzas y cuerpos de seguridad.
Como consecuencia de los hechos descritos, el servicio de salud incoó un expediente disciplinario al trabajador, que terminó con la imposición de una sanción disciplinaria, la cual fue recurrida por el sancionado ante la jurisdicción contenciosa administrativa.
En el marco del proceso judicial en que se dirimía ese recurso contencioso contra la sanción disciplinaria, el servicio de salud aportó como prueba, sin el previo requerimiento del órgano judicial, el informe relativo al reconocimiento médico practicado al empleado expedientado cuando éste fue detenido, a fin de poder acreditar su estado de embriaguez el día en que tuvieron lugar los hechos objeto de sanción disciplinaria.. Conviene resaltar sobre este informe médico, por una parte que no se había tenido en cuenta en el marco del procedimiento disciplinario, y por otra que el servicio de salud disponía del mismo en su condición de prestador de la asistencia sanitaria prestada al trabajador cuando fue detenido.
Como es obvio, el informe relativo al reconocimiento médico al que se sometió la persona detenida

- Recoger la medicación en la farmacia con receta electrónica con un historial farmacoterapéutico único que incluye la medicación administrada en el hospital.
- Consulta telefónica con su médico
- Ver directamente los informes sanitarios y de las pruebas en Carpeta de salud, Incluir notas a través de mi diario en su historia clínica (Ebook del paciente de Osabide Global)
- Participar en red social pacientes-profesionales.
- Evitar desplazamientos innecesarios al Hospital si se puede solucionar con:
  - Consultar telefónicamente con Consejo Sanitario
  - Interconsultas no presenciales entre Primaria y especializada Videoconferencia con el hospital desde su centro de referencia
  - Consultas digitales con su médico a través de la carpeta
  - Telemonitorización y seguimiento de constantes y su enfermedad lo que supone mayor implicación y corresponsabilidad.

Como ya indicó el prof. Muir (NHS), si los avances sanitarios del s. XX tuvieron como protagonistas a los profesionales sanitarios, en el siglo XXI serán los pacientes.

contenía datos de carácter personal relativos a la salud. Llegados a este punto, procede señalar que el tratamiento de los datos de carácter personal relativos a la salud, se encuentra regulado en el artículo 7 de la LOPD, al estar ante datos especialmente protegidos. El tercer apartado de este precepto determina que dichos datos de salud sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o la persona afectada lo consienta expresamente.

Ante la falta de consentimiento expreso del empleado para que el servicio de salud comunicara al Juzgado el informe que contenía datos de salud relativos a su persona, era preciso dirimir si concurría alguna habilitación legal expresa que diera cobertura al tratamiento denunciado.

En este sentido es necesario acudir a la regulación de los usos de la historia clínica, la cual viene determinada por el artículo 11 de la Ley catalana 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica; y el artículo 16 de la Ley estatal 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Analizados los usos previstos, se descartó que dicha normativa pudiera dar cobertura a la aportación de la documentación clínica al Juzgado.

En el procedimiento sancionador iniciado por esta Autoridad, el servicio de salud invocó el artículo 43 de la Constitución Española -que regula el derecho

"Los datos de salud sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o la persona afectada lo consienta expresamente"

a la protección de la salud como uno de los principios rectores de la política social y económica- como derecho que justificaría la afectación a la protección de datos de carácter personal del expedientado. Al margen de que tal invocación se realizaba de forma genérica, sin concretar quiénes eran los potenciales titulares de este derecho a proteger, se consideró que conforme la jurisprudencia del Tribunal Constitucional, el servicio de salud tenía a su alcance otras medidas menos lesivas para acreditar el estado del trabajador en el marco del proceso judicial, como pudiere ser la citación a testimonio del personal sanitario que atendió al empleado en el hospital o los agentes de policía que le trasladaron.

En definitiva, se consideró que el servicio de salud utilizó un informe que se había elaborado con motivo de una asistencia sanitaria recibida por el expedientado en un determinado hospital como consecuencia de su detención, para justificar la procedencia de una sanción disciplinaria, siendo éste un fin distinto a aquél para el que los datos habían sido recogidos.

Datos Personales de Salud y Dispositivos Móviles: "mHealth"



Ramón Miralles López
Coordinador de Auditoría y Seguridad de la Información. Autoridad Catalana de Protección de Datos

Por definición, la introducción de nuevas tecnologías de la información y la comunicación, junto con los evidentes beneficios, también implicanla concurrencia de riesgos en relación al tratamiento de los datos de carácter personal. Los riesgos en materia de procesamiento de la información deben ser gestionados, es decir, conocidos y tratados.



Cuando en el tratamiento de datos personales relacionados con la salud se ven involucradas tecnologías relacionadas con dispositivos móviles, principalmente "smarphones" y "tablets", todo y que no exclusivamente, ya que también deben ser considerados como tales todos aquellos dispositivos que incorporan características demovilidad,resulta inexcusable valorar los riesgos que concurren, y tomar decisiones en función de esa evaluación.

La gestión de riesgos implica controlar y minimizar los riesgos detectados, obviamente hasta donde sea proporcionadamente posible, aplicando la teoría general del análisis y gestión de riesgos las decisiones que se tomen se orientaran a eliminar, transferir, asumir o mitigaresos riesgos.

De la respuesta a la encuesta 2013 de TIC i Saluden Catalunya, se desprendía que el despliegue de dispositivos móviles en las entidades asistenciales se situaba en el 11por ciento del total de dispositivos de trabajo, y que un 70 por ciento de los hospitales y equipos de atención primaria disponían de ese tipo de herramientas que, con carácter general, permitían la consulta e integración

de información en tiempo real en la historia clínica electrónica.

No hay que perder tampoco de vista la consolidación de modelos de atención no presencial, es decir, de "telemedicina", ya sea para "telediagnóstico", "teleconsulta" o "telemonitorización", cuyo uso ahora se ha duplicado respecto de los datos de esa misma encuesta para el 2011, y en los que elementos característicos de los sistemas móviles están presentes, especialmente en cuanto a los aspectos vinculados a las telecomunicaciones.

El espectro de usos y tecnologías móviles es muy amplio, vamos a centrarnos aquí en el uso de dispositivos móviles en base a las denominadas "APPs",a las que genéricamente podemos referirnos como soluciones de "mHealth" o "mSalud", ya que su proliferación y uso masivo está llegando también al sector salud.

Todo y que ponerse de acuerdo sobre el número de "APPs" dedicadas al sector salud resulta complejo, ya que las funcionalidades y finalidades son muy diversas, lo cierto es que estamos hablando de la disponibilidad de varias decenas de miles de aplicaciones que,mediante "smartphones" y "tablets",están formando parte, directa o indirectamente, de procesos asistenciales y de tratamiento de información relacionada con la salud.

En la declaración de Varsovia sobre la "appificación de la sociedad", una resolución aprobaba en la XXXV Conferencia Internacional de Autoridades de Protección de datos y Privacidad, celebrada en septiembre de 2013 en Polonia, se hace referencia a que esas aplicaciones "recogen grandescantidades de datos de carácter personal. Esto permite una monitorización digital continua, a menudo sin que los usuarios sean conscientes de que esto sucede, y sin saber para qué se utilizan sus datos personales."

En un informe de finales del 2013, de "Barcelona Digital", sobre los "Riesgos de las APPS en el entorno corporativo", se identificaba como uno de los principales riesgos asociados a las "APPs" la apropiación indebida de la información, ya sea como consecuencia de la falta de medidas de seguridad, la poca granularidad de los permisos que solicitan las aplicaciones cuando se instalan o la falta de transparencia a la hora de informar sobre las finalidades y usos previstos para la información que recogen.

Estamos ante un entorno complejo, la presión por incorporar este tipo de aplicaciones viene tanto de los usuarios delos servicios de salud, como de los propios profesionales, o si lo llevamos al terreno de lo económico, por las propias áreas de gestión de los servicios.

A su vez, en el escenario de las "APPs" intervienen diferentes actores: desarrolladores, proveedores de sistemas operativos, promotores de los servicios y aplicaciones, plataformas de descarga de aplicaciones y por descontado los usuarios.

Por tanto podemos afirmar, con poco margen de error, que el entorno de las "APPs" es complejo, y esencialmente inseguro, pero aún estamos a tiempo de establecer unas reglas que, sin menoscabo de las funcionalidades propias de ese tipo de aplicaciones, protejan a los usuarios de los diversos riesgos que implica su uso.

Como ya estamos acostumbrados a presenciar, a la hora de diseñar esas soluciones, las funcionalidades y prestaciones de las aplicaciones y tecnologías se anteponen a otros criterios, como la privacidad y la seguridad, y no solo por parte de la industria, también por parte de los usuarios; se hace preciso pues, incidir en la necesidad de establecer unas buenas prácticas y unos hábitos digitales saludables que permitan discernir que aplicaciones son confiables y cuáles no.

"El despliegue de dispositivos móviles en las entidades asistenciales se situaba en el 11% del total de dispositivos de trabajo, y que un 70% de los hospitales y equipos de atención primaria disponían de ese tipo de herramientas que, con carácter general, permitían la consulta e integración de información en tiempo real en la historia clínica electrónica"

Por ello, algunas de las herramientas, que en forma de obligaciones, plantea la propuesta de Reglamento Europeo de protección de datos, pueden resultar de gran utilidad: la obligación de evaluar los riesgos para tomar decisiones sobre los tratamientos de datos personales y sobre su seguridad, "incrustar" en las organizaciones la cultura de la privacidad en el diseño por defecto, o procesos materiales de análisis de los tratamientos, basados enevaluaciones de impacto sobre la privacidad, son propuestas que sin duda favorecerán un clima de mayor confianza y uso en las "APPs" y de mitigación de los riesgos derivados de su uso.

La Tormenta (im)perfecta



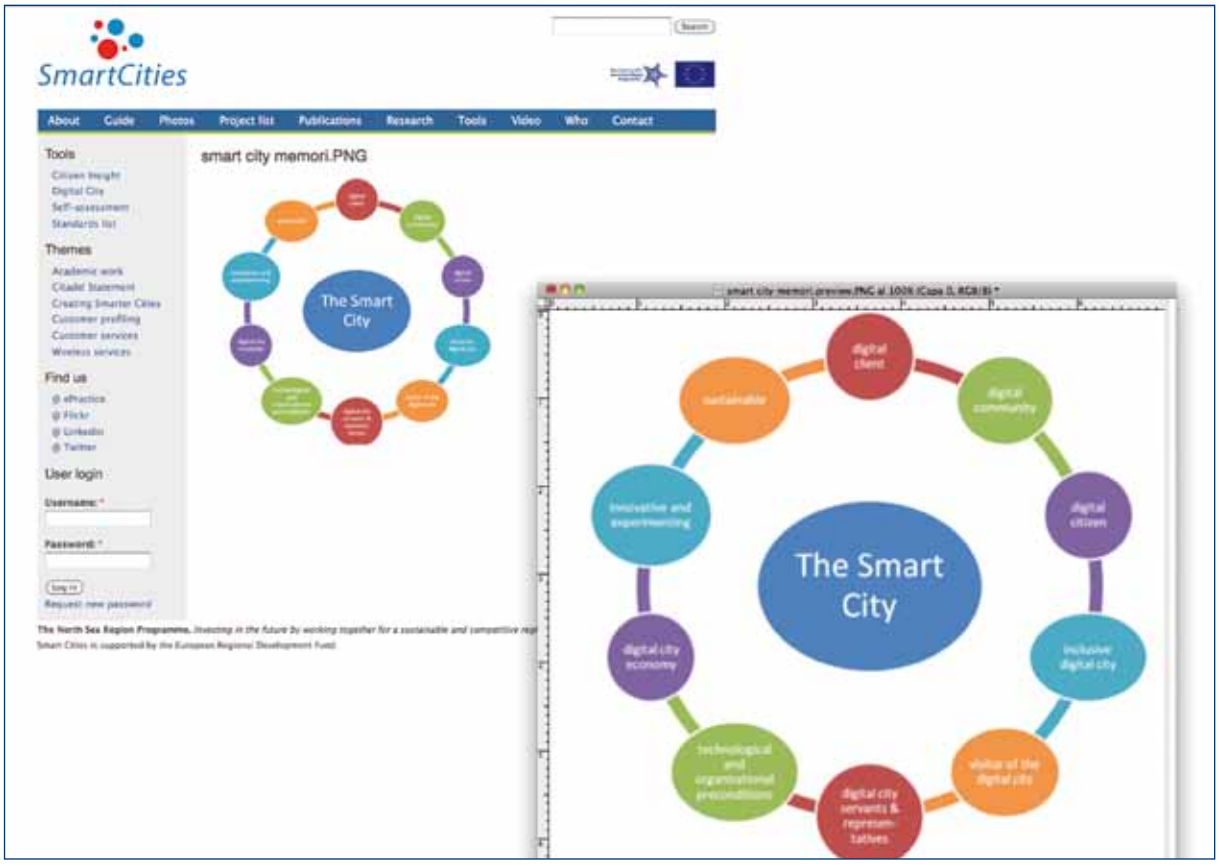
Toni Felguera
Responsable del Área de R+D+i Seguridad. Barcelona Digital

Comienza siquiera a gotear. Afuera se percibe todavía tranquilo, quizás cierta aceleración en el curso de los acontecimientos más recientes, pero ya se sabe que esta sociedad nuestra va cada vez más deprisa. A pesar de ello, ajena a tribulaciones de medio pelo, poco a poco la tempestad se cierne, visible e irremediablemente transparente para aquel que mira entre las costuras de una realidad cada vez más mediatizada por la intervención necesaria de la tecnología.

Lloverá, porque siempre llueve cuando antes chispea en el mundo de las TIC. Y esta vez parece que lloverá fuerte. Anuncian que soplan vientos húmedos de un costado, y fríos del interior del otro, el hambre con las ganas de comer, la progresiva tecno-socialización de los ciudadanos ávidos de saborear la siguiente novedad tecnológica, con la imperiosa necesidad de las marcas por crear nuevos conceptos y estrategias de consumo.

Y perdóneme Vd. si en este día de lluvia que compartimos, alguna vez peco de ingenuo y todavía utilizo el término ciudadano, quiero en realidad decir consumidor. A estas alturas, a ninguno de los dos se nos escapa en estos compases iniciales de calabobos, que las principales novedades tecnológicas a las que uno puede acceder son a menudo gratuitas. Y ya nuestras abuelas advertían, sin ni siquiera plantearse el ejercicio de adivinación meteorológica que aquí nos concedemos, que pocas cosas hay gratis en la vida o, como más recientemente de forma machacona se comenta; si algo es gratis en el mundo online, entonces el producto eres tú, o en este caso, tus datos.

No vea aquí una Verdad axiomática, más allá de la dosis de verdad que cada uno de nosotros quiera otorgarle. Más bien convenga conmigo que el



usuario se ve empujado socialmente a un consumo digital cada vez más avanzado, y que la tecnología impregna – e impregnará – cada vez más nuestra vida. Un ejemplo paradigmático lo encontramos en los smartphones de los usuarios, donde claramente tanto los dispositivos físicos como los usos individuales propuestos son más avanzados que los de las propias compañías, generando en este caso particular riesgos en materia de seguridad (tal y como mostró el informe de Barcelona Digital Centro Tecnológico, disponible en http://www.bdigital.org/es/Paginas/DetallesDestacado.aspx?xid=134), y de forma general, la sensación de que la innovación digital (sobre todo la de ámbito personal) se está convirtiendo cada vez más claramente en una cuestión de competencia y dinamización individual.

Y esto cala. Llueven datos y más datos, y no será este un episodio de chubascos aislados sino más bien un aguacero persistente. Todavía están por venir nubes cargadas llamadas "e-health/m-health", "Smart cities", "weareablecomputing", "Internet of Things", "Cloud Computing", "Linked data", que prometen más y mejores formas de obtención de datos personales y usos que nos llevaran a disfrutar de nuevos servicios aún hoy no concebidos. Y también, como no, de nuevos retos para la gestión de esos datos, y de los derechos de privacidad que de ellos se desprenden. Nunca llueve a gusto de todos. Y como en todo aguacero, es importante estar bien equipados para sobreponerse. La innovación es un motor de cambio importantísimo para el avance de nuestra sociedad, y la propuesta de nuevas y mejores tecnologías una palanca segura donde apoyarse para superar la grave crisis que estamos viviendo. Sin embargo, además en Barcelona Digital apostamos por hacer esta tecnología más humana, acercándola al servicio de los ciudadanos, preservando su carácter de medio, y no de fin en sí mismo. Es por ello que el fortalecimiento de la seguridad y privacidad de las tecnologías que desarrollamos ocupa un lugar muy importante en el proceso de desarrollo, y que hemos podido constatar que muy pocas veces se tiene realmente en cuenta.

Porque en la sociedad actual, donde la tecnología adquiere un papel importantísimo en el desarrollo de su bienestar, surgen nuevos riesgos en materia de privacidad y seguridad que son imprescindibles de considerar: la seguridad de las comunicaciones, la del propio desarrollo de las aplicaciones que generamos, la seguridad de los datos que guardamos y tratamos, la seguridad en el uso de aplicaciones de terceros, etc. Por ello, no tardarán en hacerse populares servicios que hoy ya comenzamos a prestar en Barcelona Digital, como la huella en privacidad: una evaluación del impacto que los servicios prestados generan en la privacidad de los usuarios, de la misma forma que calculamos el impacto ambiental de nuestras acciones, ayudándole consecuentemente a generar estrategias alternativas de acción más sostenibles. O la revisión de la seguridad de las aplicaciones móviles, gracias a contar con la experiencia de nuestro equipo de investigadores en el mundo de la defensa contra el cibercrimen.

Comienza a arreciar, y para ello se ha de estar bien preparado. La privacidad y la seguridad pueden llegar a convertirse en un valor competitivo esencial en un mundo globalizado que ya ha vivido episodios que cuestionan el respeto a las libertades individuales, o simplemente una necesidad esencial para poder operar en el mercado europeo, como mínimo. Urge, por tanto, abrir el paraguas de inmediato y diferenciarse, para no acabar en breve con una indeseada pulmonía.



Situación de la Movilidad en Cataluña





Francesc Moya, Jordi Martínez
Fundació TicSalut. Departament de Salut de la Generalitat de Catalunya

La aplicación de los dispositivos móviles, la movilidad, en el sector salud son nuevos canales y/o herramientas que ayudarán a implicar más al ciudadano/paciente en el cuidado de su salud , le permitirá recibir tratamientos más personalizados y ayudarána l sistema a transformar el modelo de prestación de servicios. Ayudarán a transformar el modelo de atención presencial y reactivo, a un modelo de atención no presencial y proactivo, tanto en la prevención como en el seguimiento de las enfermedades y consecuentemente contribuirán también a la sostenibilidad del sistema.

La propia evolución de la tecnología está facilitando la rápida expansión de la movilidad. Cada vez es más accesible en precio, se integra fácilmente, interoperable conotros dispositivos externos, y es más fácil de usar.

Adicionalmente, la consolidación de tecnología en la nube (Cloud Computing) facilita la implementación de servicios en movilidad permitiendo el almacenamiento remoto de información y su posterior acceso de manera compartida. Actualmente en Cataluña un 38% de los centros dicen disponer de alguna aplicación en la nube, ver figura 1. El modelo más implementado es el de nube privada y las aplicaciones más migradas son, de más a menos: el correo corporativo, alguna aplicación de negocio, las copias de seguridad y la ofimática.Son los centros más pequeños y sin grandes departamentos de Sistemas de Información los que tienden a utilizar máseste tipo de servicios.

Ante este nuevo potencial del mHealth, ¿cuál es la situación actual de su uso en Cataluña?

Según la encuesta realizada por la Fundación TicSalut, conocida como Mapa de Tendencias(1)los resultados destacables son los siguientes:

Para informar de la situación de la movilidad en Cataluña podríamos distinguir entre la movilidad aplicable a los profesionales de la movilidad destinadaal ciudadano.

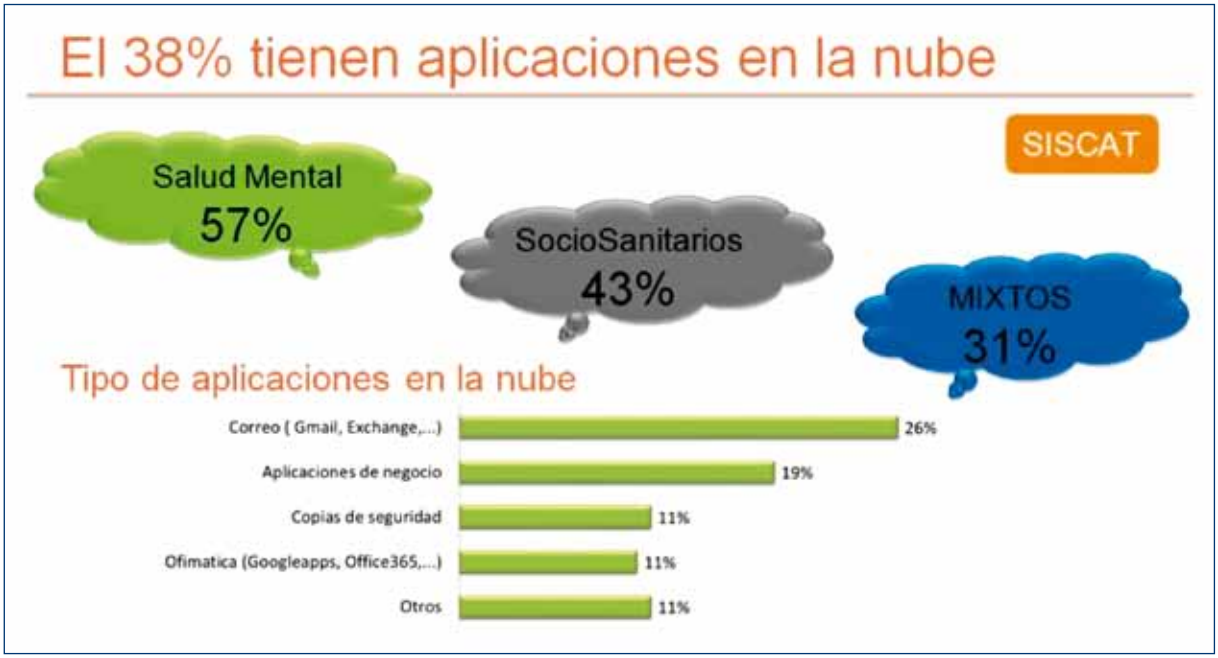


Figura 1. Utilización de la Nube



Figura 2. Situación del Registro de la Administración Hospitalaria

Centrándonos en los profesionales podríamos diferenciar entre la movilidad que se aplica dentro de los recintos asistenciales y la movilidad cuando el profesional está desplazado fuera del recinto asistencial. Actualmente hay una media de 0,80 dispositivos en general, entre dispositivos fijos y no fijos, por personal asistencial, y de estos un 11% son dispositivos móviles; cifra que a lo largo de estos años parece incrementarse muy lentamente, solo un 1% en los tres últimos años.

La mayor parte de los centros, un 70%, ya disponen de una red wifielevándose hasta un 82% en el caso de los hospitales; pero con una cobertura física de la señal por debajo del 50% de la superficie del recinto y solo un 10% declaran disponer de una cobertura del 100%.

La aplicación actual de esta movilidad interna va muy ligada a herramientas de trabajo de los equipos directivos y a los pases de visita en planta, en concreto y fijándonos en la figura 2, un 36 % de las unidades de enfermería disponen de un Registro Electrónico de la Administración de la Medicación a pie de cama del paciente.

Actualmente se observa poca presencia de Smartphones de empresa, en términos de volumetría, si bien un 70% de los centros declaran disponer de ellos. Su uso es mayoritariamente para comunicarse (hablar, correo electrónico,…) y para el uso de Apps de terceros; solo un 10% de los centros utilizan Apps específicas de negocio y 3 centros declaran hacer uso de Apps propias.

Un 24% permiten que se utilicen/conecten los propios dispositivos de los trabajadores (tabletas, smartphones…) siguiendo la tendencia internacional denominada BYOD (BuyyouronDevice).

Respecto al uso de la movilidad fuera del recinto asistencial, en promedio, un 70% de los equipos de atención a domicilio declaran trabajar con dispositivos móviles que les permite el acceso remoto a la HistóriaClinica Electrónica, ver figura3.

ATENCIÓN DOMICILIARIA Y DISPOSITIVOS MÓVILES

Una media del 60% de los centros permiten el acceso a su datos desde portátiles, un 32% desde tabletas y un 18% desde smartphones.

En relación a los ciudadanos, cada vez más digitali-

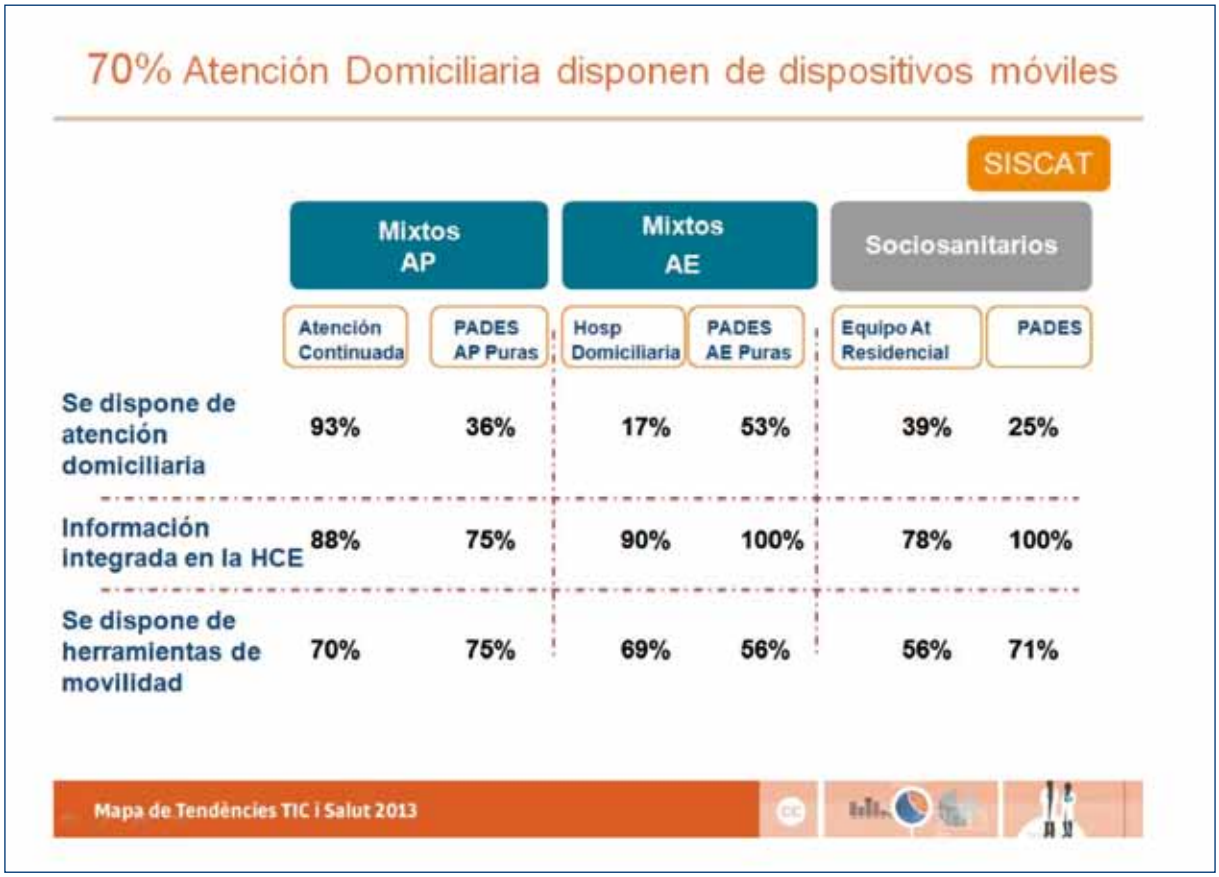


Figura 3. Situación atención a domicilio

zados, los centros empiezan a ofrecerles una serie de servicios, entre los que podemos destacar:

- un 25% de los centros les facilitan poderse conectar a internet dentro del recinto asistencial
- Entre un 33%, ámbito general, y un 53%, ámbito hospitalario, les envían recordatorio de visitas vía SMS e incluso un 5% llegan a notificar resultados.
- 1 centro en este 2013 afirma estar prescribiendo Apps de terceros e incluso Apps propias.

Por tanto, desde un punto de vista institucional, el uso es incipiente. El mHealth facilita al ciudadano poder realizar un doble rol desde el punto de vista de la información: ser consumidor (mejor informado, más conocimiento de su enfermedad) y ser generador (más participación/implicado). Uno de los puntos fuertes y diferenciadores de la movilidad aplicada al ciudadano es que es un dispositivo individual y por tanto se le pueden incorporar funcionalidades/aplicaciones personalizadas que le ayuden a gestionar/prevenir mejor su enfermedad, de aquí el gran volumen de Apps que están apareciendo. El reto será solucionar la fiabilidad de dichas Apps mediante un sistema de homologación/certificación, así como su evaluación eintegración con los sistemas corporativos (Historia Clínica Compartida y/o Canal Personal del Paciente), sus modelos de negocio y su seguridad en su globalidad.

Comentar que los datos obtenidos del Mapa de Tendencias(1)de la Fundación TicSalutson a partir de las respuestas facilitadas por los mismos responsables de Sistemas de información de los centros asistenciales en la encuesta 2013, realizada entre septiembre y octubre de 2013.

FUNDACIÓN TICSALUT

La Fundación TicSalut, con el objetivo de conocer objetivamente el nivel de adopción de las TIC en las organizaciones sanitarias de Cataluña, lleva a cabo anualmente, desde el año 2007, y por encargo del Departamento de Salud, la encuesta Mapa de Tendencias en TIC y salud, un documento de referencia para el sector sanitario, que aporta una visión de la realidad, a nivel de implementación, uso y evolución de las TIC en la red de centros sanitarios públicos catalanes (atención primaria, hospitalaria, socio-sanitaria y salud mental) (http://www.ticsalutcat/observatori/es_enquesta-tic-salut/).

Mensajería Instantánea para Uso Clínico



M. Àngels Calvet Canaleta
Responsable de la Oficina de Mobilitat GTMN (Gerencia Territorial Metropolitana Nord)

La mensajería instantánea para uso clínico requiere mecanismos de seguridad para validar su uso en decisiones sanitarias cumpliendo los preceptos de la LOPD. Los programas actuales no cumplen las condiciones necesarias para adoptar dichas soluciones. Una opción a estudiar es la liberación del código del servidor, tal como ha enunciado Telegram en cuyo caso se podría disponer de una solución 100% controlada.

COMPARACIÓN EN TÉRMINOS DE SEGURIDAD DE LAS FUNCIONALIDADES DE 3 APLICACIONES MENSAJERÍA CORTA

En el caso de los programas de mensajería corta, según trecebits.com los actores más importantes del mercado son WhatsApp con 465mill de usuarios registrados, seguido por Line con 360mill, WeChat con 320mill, Viber con 280mil y Telegram con 100millones y según la tabla telegram es la más segura. Pero, a pesar del convencimiento que demuesta telegram en la Seguridad de su aplicación al estar ofreciendo un premio o recompensa de $200, 000 en bitcoins a quien demuestre lo contrario, hemos de ser determinantes aplicando la normativa española que establece la Ley Orgánica de Protección de Datos (LOPD). En el caso que nos ocupa, una teleconsulta, observamos que 2 de las 7 consideraciones que hay que tener en cuenta al aplicar la LOPD no se cumplen y son:

1. Se tiene que conocer dónde se almacenan los datos físicamente
   En Telegram se desconoce oficialmente donde están almacenados los datos
2. La ruta que siguen los datos tiene que ser trazable.

Telegram enruta la comunicación hacia un cloud propio.

Es por ello, que actualmente no tenemos una solución fiable para la mensajería instantánea para uso clínico.

Pero, telegram ha dado el paso de liberar el protocolo y el código fuente de sus clientes Android y iPhone también ha anunciado la liberación del código del servidor durante el 2014. La reacción no



se ha hecho esperar: Ya hay versiones de escritorio para Windows y Mac, además están disponibles librerías Java para implementar soluciones en el repositorio https://github.com/ex3ndr/telegram-api.

PRECEDENTE: OPENSIM Y SECONDLIFE

En 2003 hizo su aparición Second Life, un entorno virtual tridimensional desarrollado por la compañía Linden Labs en el que los usuarios participan en él mediante un avatar que controlan ellos mismos. Técnicamente se pueden identificar dos partes: la parte cliente, que se manifiesta como un visor o "player" del entorno virtual, y por otro lado la parte servidora, que almacena los entornos y ejecuta las reglas de operación. El cliente y el servidor se comunican mediante un protocolo, que define con precisión el conjunto de mensajes y el formato de cada uno de ellos entre las dos partes.

"Estamos a la espera de que telegram libere el código servidor para así implementar nuestra solución e incorporar la solidez de los mecanismos de seguridad en soluciones sanitarias cumpliendo los preceptos de la LOPD"

Es precisamente en 2007 cuando Linden Labs hace público el protocolo libre de licencia. La noción de protocolo es clave ya que una vez especificado hace técnicamente posible que puedan desarrollarse diversidad de visores compatibles y también diversidad de servidores, de modo que pueden darse todas las combinaciones clientes entre clientes con servidores, dando lugar ricos ecosistemas de componentes que compiten y cooperan entre sí al mismo tiempo.

Tras la liberación del protocolo, se iniciaron en paralelo varios desarrollos de visores para diversos sistemas operativos y escritos en diversos lenguajes, como Firestorm, Imprudence o Lumiya para Android, varios de ellos en régimen abierto. También empezó el proyecto OpenSim, un servidor open source escrito en C# de Microsoft compatible con la máquina virtual MONO lo que permite su ejecución tanto en entornos Windows como Linux. Ello permite que una organización pueda instalar, y en el caso de código abierto, incluso adaptar una solución propia, en entornos de ejecución propios como servidores físicos o prívate Cloud y Apps para la parte cliente, disponiendo de una solución que denominaremos 100% controlada. Es esperable, pues, que ya sea por la liberación del código fuente por parte de telegram, o bien por la aparición de uno o más proyectos abiertos de implementación de la parte servidora podamos disponer de una base para una solución 100% controlada durante 2014.

CONCLUSIÓN

Podemos concluir diciendo que estamos a la espera de que telegram libere el código servidor para así implementar nuestra solución e incorporar la solidez de los mecanismos de seguridad en soluciones sanitarias cumpliendo los preceptos de la LOPD. A partir de una solución 100% controlada, quedaría como tarea pendiente incorporar nuestros certificados digitales de confianza como base de los mecanismos de criptografía.

BIBLIOGRAFÍA

- Comparativa: WhatsApp, Line y Telegram [Infografía].
[Consulta URL el 13 de Marzo de 2014]. Disponible en: http://www.trecebits.com/2014/03/03/comparativa-whatsapp-line-y-telegram-infografia/

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[Consulta URL el 13 de Marzo de 2014]. Disponible en: http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t2.html#a8

- Guías y recomendaciones de la agencia española de protección de datos.
[Consulta URL el 13 de Marzo de 2014]. Disponible en: https://www.agpd.es/portalwebAGPD/jornadas/dia_proteccion_2011/responsable/guias-ides-idphp.php

- Telegram Java Libraries
[Consulta URL el 13 de Marzo de 2014]. Disponible en: https://telegram.org/apps https://github.com/ex3ndr/telegram-api

- #Telegram: uso clínico, seguridad y legislación aplicable.
[Consulta URL el 13 de Marzo de 2014]. Disponible en: http://www.perdidosenpandora.com/2014/03/telegram-uso-clinico-seguridad-y.html

La Práctica de la Medicina en Tiempos de Multimorbilidad y Big Data



Roberto Nuño-Solinís
Director de O+berri, Instituto Vasco de Innovación Sanitaria

La tensión entre especialización y generalismo es un elemento recurrente de la medicina moderna. La evolución hacia una hiperespecialización ha conformado una especie de profecía autocumplida en un sector orientado a la enfermedad y no a la salud.

Sin embargo, el auge de los modelos de crónicos y la problemática de la multimorbilidad han servido para poner en valor la Atención Primaria y recuperar el generalismo médico con interesantes iniciativas de trabajo en procesos integrados entre especialidades de medicina de familia, internistas y geriatras.

La multimorbilidad es la norma y no la excepción en nuestras envejecidas sociedades, pero seguimos generando conocimiento clínico con el paradigma de la enfermedad única, aislada, "pura". Un sinsentido, cuando la práctica cotidiana se caracteriza por personas añosas con patologías múltiples, y problemas sociosanitarios muchas veces complejos. Esos pacientes son sistemáticamente excluidos de los ensayos clínicos, donde se genera conocimiento cada vez más alejado de la realidad de la práctica profesional.

El énfasis en la visión holística de la persona, en la personalización de la atención y el cuidado, ha de balancearse con la necesaria estandarización y homogeneización de la información y la reducción de la variabilidad innecesaria. El elevado número y creciente complejidad de los elementos de información a considerar en el diagnóstico y tratamiento de las personas excede con mucho los conocimientos personales y capacidades analíticas que cabe exigir a los profesionales médicos, por mucho que estemos ante uno de los paradigmas de "trabajadores del conocimiento".

Sin embargo, persistimos en confiar en una cultura de atención y cuidado idiosincrática y poco normalizada, con un grado de variabilidad inaceptable y con una subutilización del enorme caudal de información acumulado sobre pacientes individuales y poblaciones. La explotación y utilización sistemática de esa información permitiría dotar al profesional de herramientas soporte a la decisión médica, así como conocer el impacto real de los tratamientos a nivel poblacional. Más aún, herramientas de modelización predictiva, nos permitirían actuar de forma proactiva y preventiva. Sólo unos pocos sistemas sanitarios líderes están apostando por estas líneas de trabajo. En la mayoría de los casos, las enormes barreras legales y organizativas, acompañadas de la imparable marea del status quo, sirven de motivaciones y excusas para no acometer estos necesarios cambios.

Necesitamos modelos de organización y métodos de trabajo con un uso intensivo de herramientas tecnológicas para conectar sistemáticamente datos de los pacientes con conocimientos biomédicos y proporcionar información útil para la decisión del (equipo) médico. De la cual no puede ajenizarse al paciente, ya que las alternativas van a ser crecientemente variadas no dictadas únicamente por las circunstancias del (escaso) tiempo de consulta, ni por una evidencia "estándar" sacralizada ni por la personalidad del proveedor… siendo necesario un modelo más compartido y participativo de relación entre el paciente y los profesionales sanitarios.

El advenimiento del big data en una cultura profesional plagada de variabilidad inaceptable no augura los beneficios que cabría esperar en un escenario más ordenado. En nuestro medio, Peiró y Bernal han mostrado como para algunas pruebas y tratamientos no es infrecuente que las tasas de utilización (estandarizadas por los confundidores de interés) varíen cinco, diez y más veces entre poblaciones vecinas sujetas a condiciones de entorno y morbilidad similares.

El sistema sanitario ha de avanzar en la sistematización de las formas en las que evaluamos a los pacientes, en las formas en que hacemos coincidir sus datos con nuestra base de conocimientos existente, y en la forma en que documentamos nuestros procesos clínicos. Sobre esa base sólida y consistente de información y conocimiento que aproveche las posibilidades de computación existentes, y que minore la incertidumbre del proceso, cabe erigir un modelo de atención que emplee el juicio clínico como navegador sobre esos inputs de conocimiento y con flexibilidad suficiente para adaptar la actuación clínica a las preferencias del paciente y a las circunstancias individuales.

Implementar en la práctica un modelo de encuentro clínico y de organización del sistema de prestación que conjugue el potencial de la explotación sistemática del big data, permita conjugar conocimiento poblacional con características individuales, se adapte a las preferencias y realidades de cada persona supone un verdadero reto para el cual solo contamos con incipientes esbozos, pero que debe ocupar un lugar preeminente en todas las agendas de innovación sanitaria.

Ippok Comunidad Sanitaria, nuevo entorno de Intercambio de Información en Salud



Rosario Serrano
Directora Gerente del Área de Salud. Unidad Editorial. Diario Médico, Correo Farmacéutico e Ippok

Creo que la mejor forma de empezar este artículo es hacerse una pregunta clave, ¿por qué y para qué IPPOK? En primer lugar, decir que IPPOK es la red social de profesionales sanitarios de Diario Médico y Correo Farmacéutico. Es una red vertical de entorno cerrado con conversación y contenidos por y para el profesional.

IPPOK nace a mediados del 2012 con el objetivo de posicionarse como la comunidad de referencia de los profesionales del sector:médicos, farmacéuticos, enfermeros y otras profesiones de habla hispana.

Con nuestra experiencia de éxito durante 20 años en el papel, 15 en las webs (www.diariomedico.com y www.correofarmaceutico.com) y la suma de la aparición de nuevos avances tecnológicos como las RRSS , teníamos los ingredientes suficientes para sumar a nuestro liderazgo un paso más, el de la conversación.

Cuando diseñamos el producto digital contamos con lo más importante, la opinión en primera persona de los protagonistas de la conversación, nuestros usuarios. Para ello, llevamos a cabo dos FocusGroup con los influencers del momento, tanto del mundo médico como del mundo farmacéutico. Les preguntamos cómo querrían que fuera su comunidad y a partir de esas conclusiones nos pusimos manos a la obra.

En mi opinión, lo más destacable fue que todos ellos coincidieron en que solo participarían en un tipo de comunidad así, siempre y cuando se garantizara un entorno seguro, es por tanto, una sorpresa inicial ya que por aquel entonces el boom de las redes sociales era la de compartir de forma abierta y libre sin limitaciones. Eso nos planteaba un hándicap pero por el contrario, una oportunidad clara de diferenciación, la famosa USP (UniqueSellingProposition).

MEDIDAS DE SEGURIDAD ADOPTADAS

Así, dentro de este nuevo escenario de intercambio de información en salud, los profesionales demandaron una seguridad en el acceso y navegación de la comunidad. Por este motivo, adoptamos un conjunto de medidas que nos ayudaron a crear la plataforma que los profesionales demandaban.

La primera medida fue la definición de un estricto proceso de registro con certificación por varias vías que nos llevó a desarrollar servicios web para la validación de usuarios.

Lo segundo que había que garantizar era la privacidad en los diferentes escenarios integrados dentro de la Comunidad online. De este modo, definimos funcionalidades generales para crear un marco informático y estudiamos posibles limitaciones creando un estricto sistema de permisos de participación y publicación de contenido dentro de la Comunidad. La interacción base tiene como nexo de unión las especialidades y los usuarios tienen acceso compartido a herramientas de trabajo colaborativo, trabajos y documentos.

Respetamos la intimidad de los visitantes de nuestra comunidad, considerando de gran importancia la protección de la misma.

Recogemos datos personales únicamente cuando son voluntariamente facilitados por su titular a través de la página web de la comunidad. Los datos facilitados podrán ser utilizados para comprobar su condición de profesional sanitario, para mejorar nuestro nivel de servicio o el contenido de nuestra página web y para responder a sus consultas.

El objetivo es crear un entorno seguro en el que el profesional sanitario pudiese relacionarse a dos niveles: el social o cotidiano y el profesional vinculado al diagnóstico y la práctica.

A día de hoy, contamos con 13.000 usuarios registrados y seguimos creciendo y evolucionando día a día, gracias a la participación de nuestros usuarios.

PREOCUPACIÓN DEL USUARIO POR LA PRIVACIDAD

El miedo por la privacidad en los usuarios online es cada vez mayor y este miedo se intensifica cuando hablamos de sectores específicos como el caso del sector sanitario.
Los usuarios se muestran cada vez más contrarios a proporcionar sus datos de carácter personal y profesional en los nuevos escenarios online de interacción. La desconfianza y preocupación del usuario es creciente y el usuario exige mayores medidas y certificados de calidad antes de facilitar sus datos o participar en una página web.

REGULACIÓN SOBRE PRIVACIDAD

El usuario cada vez es más consciente de la pérdida decontrol de su privacidad y esto genera una actitud de recelo. Existen diferentes regulaciones sobre la materia en función del país.En Europa,por ejemplo, la legislación reconoce la privacidad como un derecho y se exige a las marcas que pidan consentimiento a sus usuarios. En el caso de

"Los usuarios se muestran cada vez más contrarios a proporcionar sus datos de carácter personal y profesional en los nuevos escenarios online de interacción. La desconfianza y preocupación del usuario es creciente y el usuario exige mayores medidas y certificados de calidad antes de facilitar sus datos o participar en una página web"

EE.UU la regulación es distinta.A pesar de estas diferencias, todas las iniciativas online podrían perder su valor principal, el usuario, si no proporciona desde el comienzo, la transparencia que el usuario demanda.
El usuario debe tener siempre laopción de elegir, decidir qué es lo que quiere hacer y controlar sus datos personales en todo momento. Del mismo modo, el usuario debe ser capaz de controlar e influir en la recogida y almacenamiento de datos relativos a ellos mismos, así como por quien y a quien pueden ser dados a conocer estos datos.



En Busca de una Industria más Competitiva a través de la Investigación Europea en Seguridad TIC



Sofía Moreno Pérez
Miembro del equipo de FIRE

El proyecto europeo FIRE tiene como objetivo facilitar que los resultados de la investigación europea en seguridad TIC se transformen en oportunidades reales para la industria y tengan un impacto directo en la sociedad.

Europa lleva años invirtiendo en investigación a través de programas que hasta ahora han recibido el nombre de Programas Marco. El pasado diciembre se lanzó el nuevo programa de ayudas a la investigación para el periodo 2014 - 2020 con un nombre renovado, Horizon 2020, y un presupuesto cercano a los 70.000 M€. Todos estos esfuerzos por impulsar la I+D+i europea han propiciado la consolidación de grupos de investigación de excelencia internacional en muchas áreas, incluyendo la seguridad TIC. Sin embargo, Europa sigue teniendo como asignatura pendiente que los resultados de la investigación se conviertan en oportunidades para la industria y que de esta manera generen un impacto palpable en la sociedad.

Mejorar la competitividad de la industria europea a través de la investigación se ha convertido en el punto de partida del Horizon 2020. El proyecto FIRE es una de las iniciativas que ha comisión europea ha puesto en marcha para contribuir a esta mejora. FIRE es acrónimo de *Facilitating Industry Research in Europe*, - Facilitando la Investigación Industrial en Europa, en español -. Esta iniciativa busca generar prioridades de investigación en seguridad TIC que sean financiadas en próximas convocatorias del programa Horizon 2020, así como recomendaciones para elevar su impacto en el mercado. Para ello, FIRE aborda su estudio desde varias perspectivas. Una de ellas parte de analizar las necesidades específicas en seguridad TIC de cuatro sectores estratégicos: salud, energía, móviles y finanzas. Estas necesidades son contrastadas con la visión de la industria y de los investigadores europeos para identificar posibles oportunidades de trabajo conjunto. En este momento el trabajo está en marcha y los resultados obtenidos durante el primer año están siendo presentados en foros, como el de la SEIS, donde expertos en las diferentes materias pueden aportar su visión.

A continuación se expone un resumen de las conclusiones de FIRE respecto a las necesidades del sector Salud obtenidas hasta el momento:

- Crear un **marco legal y de interoperabilidad europeo** en cuanto al tratamiento de los datos de salud en los nuevos escenarios, que sea fácil de entender y de implementar por la industria del sector.
- **Prevenir las pérdidas de datos, masivas o de individuos**. ¿Cómo de difícil es conseguir la información de una persona cuando tantas pueden acceder a ella? Hay tecnologías para prevenirlo como el cifrado, la autenticación, etc., pero no siempre los procedimientos están bien ajustados y es difícil protegerse ante la fata de concienciación o la mala intención del personal interno. Las empresas asociadas y la monitorización remota abren nuevas debilidades.
- **Sistemas de control de acceso a los datos basado en roles/recursos.** Cada profesional que accede a los datos de un paciente debería acceder tan solo a aquellos que necesita y esto debe gestionarse de forma ágil, eficiente y segura.
- **Mecanismos de trazabilidad y auditoría.** Los sistemas de salud necesitan compartir de forma muy dinámica información sensible entre varias partes autorizadas y al mismo tiempo proteger esa información. Esto incluye a las empresas asociadas con varios niveles de subcontratación de servicios.
- **Mejora de los mecanismos de anonimización de datos**. El uso secundario de los datos de salud anonimizados abre oportunidades de investigación y de optimización de recursos y servicios excelentes, pero los mecanismos de re-identificación pueden suponer un peligro para la priva-

cidad. Es un problema dinámico que exige una revisión permanente de la tecnología, las leyes y los procesos utilizados.

- **Cloud computing** engloba varios conceptos de computación y todos ellos implican un gran número de computadores conectados a través de una red en tiempo real (típicamente internet). Es muy difícil saber si el proveedor (y sus subcontratados) tienen las instalaciones y políticas adecuadas. A veces es difícil saber donde están y qué legislación les aplica. Conforme el cloud se haga más popular la ciber delincuencia explotará cualquier debilidad.
- **Mecanismos de auditoría de protección de datos en móviles y BYOD** (*Bring your own device*). Detección de pérdidas de datos. La penetración creciente de dispositivos móviles genera riesgos de pérdidas, robos y de accesos indebidos en terminales desatendidos. Es una vía de entrada para el código malicioso y además las transmisiones inalámbricas domésticas o públicas no siempre son suficientemente seguras.

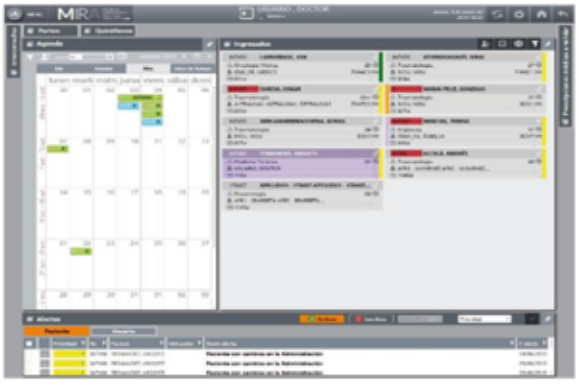
"Mejorar la competitividad de la industria europea a través de la investigación se ha convertido en el punto de partida del Horizon 2020"

- **Desarrollo de mecanismos para la implementación efectiva del consentimiento informado en los nuevos entornos distribuidos.** Los ciudadanos somos dueños de nuestros datos y podemos usarlos y compartirlos para mejorar nuestro cuidado. Pero ¿somos conscientes del alcance de nuestras acciones en el mundo digital? ¿Cómo podemos revocar permisos sobre sistemas distribuidos?

Toda la información pública elaborada por el proyecto está disponible en www.trustworthyictonfire.com y los comentarios a la misma son bienvenidos en sofia.moreno@trustworthyictonfire.com



SAVAC Consultores
MEDICAL APPLICATIONS SUPPORT



Si ya tienes tu HIS y sólo necesitas actualizar o instalar las estaciones de trabajo clínicas, MIRA® como te podemos ayudar:



Con una herramienta con funcionalidades diseñadas sólo para el trabajo de los asistenciales (tanto parte médica, como enfermería), que te dará alertas personalizadas de los sucesos mas relevantes y te permitirá realizar la prescripción (farmacológica y no farmacológica), la administración y la realización de tareas de enfermería y planes de cuidados, y que además se **integra con cualquier sistema de información asistencial** a través de los estándares: XML,HL7,DICOM,SNMP y normas UNE

MIRA® (Medical Integration Realtime Architecture) es la solución de SAVAC para las estaciones clínicas de trabajo.

SAVAC CUIDANDO A LOS QUE NOS CUIDAN

Entrega de los Premios SEIS 2013

Como es habitual el pasado 22 de enero la SEIS reunió en el salón de actos de la facultad de Medicina de la UAM a socios y profesionales del sector para proceder al acto más entrañable de todos los que organiza la SEIS.



"La Sociedad Española de Informática de la Salud comienza cada año con el acto de entrega de los Premios Nacionales y Salud, y esto no es una casualidad. Lo hacemos, en primer lugar, porque estamos convencidos de que uno de los aspectos más importantes para apoyar los objetivos de la SEIS es, promocionar la implantación de las TIC en la atención sanitaria como factor de calidad, de mejora continua y de un mejor y más racional uso de los recursos existentes, reconocer a todos aquellos profesionales y organizaciones que se han distinguido a lo largo del año anterior por su excelencia en la consecución de estos objetivos.

Pero, además, entendemos que es bueno comenzar el año con optimismo y esperanza, optimismo y esperanza que nos transmiten todos los premiados con su trabajo bien hecho y con su compromiso con la mejora del sistema sanitario español". Con estas palabras inició el acto **Emilio Aced**, secretario general de la Sociedad Española de Informática de la Salud, quien coordinó y presentó este acto anual.

Entre sus palabras destacamos su agradecimiento por participar en este acto a **Juan Antonio Vargas** Núñez, decano de la Facultad de medicina de la UAM, que generosamente ofreció su hospitalidad e hizo posible que estuviésemos reunidos en este magnífico entorno académico y científico. Agradeció la presencia de **Francisco Fernández,** director de Correo Farmacéutico y Diario Médico; **Mª José Marzal,** directora de ComputerWorld; Juan Fernando Muñoz Montalvo, subdirector general de Tecnologías del Ministerio de Sanidad, Servicios Sociales e Igualdad, y a **Javier Olave Lusarreta**, vicepresidente de la Asociación de la Prensa de Madrid.

Así mismo destacó la labor de **José Luis Carrasco,** profesor, que durante dieciocho años se ha encargado brillantemente de organizar y presentar esta entrega de premios y manifestó que gracias a su ayuda y apoyo había sido posible que todos los que habían participado en esta tarea la pudieran llevar a cabo. También agradeció todo el apoyo y la ayuda recibida de la Secretaría Técnica de la SEIS.

En su intervención, el decano de la Facultad de Medicina de la UAM dio la bienvenida a todos los presentes en el Salón de Actos de la UAM y continuó con estas palabras: "Nuestra Facultad, como institución, se encuentra honrada de poder albergar este acto y en nombre de todos los que la componemos, quiero felicitar a los premiados por su esfuerzo continuado y por su tesón en la búsqueda de soluciones tecnológicas en el sector sanitario. Además, entre los premiados se encuentra este año nuestro querido Prof. Carrasco, profesor de Bioestadística en esta Facultad durante muchos años y maestro de ceremonias habitual de este acto. Querido José Luis, muchas gracias en nombre de todos por tu generosidad. Como todos Vds. saben las TIC representan un elemento clave en la atención sani-

taria, aunque todavía hay mucho por desarrollar. En el contexto actual de crisis económica es preciso apostar por el desarrollo de las TIC que son capaces de mejorar la atención de nuestros pacientes, facilitar la labor a los profesionales y por lo tanto, seguir avanzando en la modernización y mejora de nuestro sistema sanitario. Como decano reitero mi apoyo a la Sociedad Española de Informática de la Salud representada por su presidente Luciano Sáez, y queremos seguir colaborando estrechamente como hasta ahora."

Luciano Sáez Ayerra, presidente de la Sociedad Española de Informática de la Salud, agradeció al decano su apoyo y colaboración y felicitó a los galardonados por su esfuerzo en el impulso de las TIC en el sector sanitario: "Es importante reconocer el trabajo realizado a las autoridades, directivos y profesionales que han sido destacados en esta XIX edición de los Premios Anuales de la SEIS. Esperamos aportar un pequeño aliciente personal o institucional por su labor para la innovación de nuestra sanidad. Son un estímulo para todos los que les acompañamos hoy y creemos que es el valor que las TIC pueden aportar a nuestro sistema nacional de salud. Estos premios son una muestra de lo mucho y bien que se trabaja en nuestro sector".
Así mismo dedicó unas palabras a **José Luis Carrasco.** "No puedo perder la ocasión para agradecer públicamente a José Luis Carrasco su dedicación y buen hacer durante más de 35 años en la Sociedad Española de Informática de la Salud, como miembro destacado de la junta directiva y que finalizó, a petición propia, el pasado año, según sus palabras, para dar paso a nuevas generaciones impulsoras de la innovación. No voy a exponer sus muchas acciones en la sociedad pero sí voy a destacar algunas por su relevancia: la creación de estos premios y la regularización del funcionamiento de la SEIS mediante sus Estatutos. Muchas gracias José Luis, sabemos que seguimos contando con tu ayuda". Tras su tradicional exposición sobre las actuaciones de la Sociedad Española de Informática de la Salud el pasado año y las acciones previstas para 2014, finalizó agradeciendo la presencia de autoridades, directivos, representantes de asociaciones, de la industria, profesionales del sistema sanitario y tecnológico. "Es muy importante que en sus diferentes ámbitos profesionales apoyen e impulsen una renovación de los procedimientos sanitarios. Las TIC son el instrumento que permite esta renovación del sistema de salud y debe ser la plataforma para aplicar medidas que garanticen la sostenibilidad del sistema mejorando, a su vez, el acceso a la equidad, seguridad, la continuidad y la calidad de los servicios sanitarios".

Seguidamente, **Emilio Aced** procedió a la lectura del Acta del Jurado de los XIX Premios Nacionales de Informática y Salud y a la entrega de galardones. Constituido el jurado de los XIX Edición de los Premios Nacionales de Informática y Salud 2013, formado por los miembros de la Junta Directiva de la Sociedad Española de Informática de la Salud, decidió la concesión de los siguientes premios:

1. Premio Nacional de Informática y Salud 2013, a la Entidad Pública o Privada que ha destacado en la implantación y uso de las Tecnologías de la Información y la Comunicación en el ámbito sanitario. Premio concedido al Servei de Salut de les Illes Balears, por su Programa de Atención al Paciente con Enfermedades Crónicas (PAPEC), proyecto que mejora la eficiencia en la atención sanitaria de los pacientes crónicos (EPOC y Riesgo Vascular) mediante la utilización de herramientas informáticas de ayuda a la toma de decisiones, proporcionando una plataforma común de trabajo que facilita la comunicación interniveles asistenciales y el trabajo multidisciplinar. A través de ella es posible una



Luciano Sáez Ayerra, presidente de la SEIS.



Francisco Fernández entrega el premio a Miquel Tomas Gelabert.

mejor utilización de los recursos para afrontar el aumento de la carga asistencial proveniente de las enfermedades crónicas, que ha sido posible gracias al estrecho trabajo entre expertos clínicos y tecnólogos y que ha servido de modelo para la estrategia de crónicos del SNS.



Carlos de Luis recoge el premio de manos de Javier Olave.



Losé Luis Carrasco recoge el premio de manos de LucianoSáez.

Entregó el Premio **Francisco Fernández,** director de Correo Farmacéutico y Diario Médico y lo recogió **Miquel Tomàs Gelabert**, director general del Servicio Balear de Salud. El galardonado recogió el premio y en nombre del Consejero de Sanidad de las Islas Baleares y en el suyo propio agradeció a los profesionales sanitarios e informáticos que han trabajado estrechamente en estas tares, por el esfuerzo en algo que "para nosotros ha sido muy importante y que es esta apuesta de las TIC y, por tanto, agradecerlo porque los grandes beneficiados de esto van a ser nuestros pacientes".

2. Premio Nacional de Informática y Salud 2013, a la Organización que ha realizado un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario. Concedido a Sanitas - Servicio de Promoción de la Salud, por su proyecto VITA Plataforma Tecnológica para la Promoción de la Salud que es una solución TIC del Servicio de Promoción de la Salud de Sanitas enfocada al cuidado de la salud de pacientes crónicos y de programas de promoción de la salud. Es una herramienta multicanal que ha beneficiado a más de 100.000 pacientes con unos altísimos niveles de satisfacción y que ha permitido ofrecer en cada momento la mejor opción terapéutica o preventiva. Entregó el premio **Javier Olave Lusarreta**, vicepresidente de la Asociación de la Prensa de Madrid y lo recogió **Carlos de Luis,** director de Trabajo Colaborativo – Sistemas de Información. Sus palabras fueron de agradecimiento para la SEIS por todo su esfuerzo para la aplicación de las TIC en Sanidad y también de felicitación a todos los participantes y candidatos. También tuvo un recuerdo para todos sus compañeros que habían hecho posible que se encontraran recogiendo el premio. Finalizó animando a todos para que sigan desarrollando sistemas válidos para el mundo de la salud.

3. Premio Nacional de Informática y Salud 2013, al profesional que, por su trayectoria y dedicación, ha colaborado especialmente en la implantación de la Informática en el entorno sanitario. Concedido al **José Luis Carrasco De La Peña**, doctor en Ingeniería y en Medicina, profesor universitario de Electrónica y pionero de la Bioestadística en España y profesor en esta facultad de Medicina de esta materia durante treinta años. Fue creador de un centro de investigación biomédica en el que ha desarrollado herramientas tecnológicas para soporte la investigación y poseedor de otros muchos méritos que todos conocen. Entregó el premio **Luciano Sáenz Ayerra,** presidente de la SEIS. El Profesor **Carrasco** leyó unas emotivas líneas enumerando las principales etapas de su vida profesional: "Tras unos años de enseñar electrónica en la Escuela de Ingenieros mientras me hacía médico, una mañana en 1973 me desperté sentado en un despacho de IBM con la misión de hacer sentir lo imprescindible que eran las nuevas tecnologías y difundir y organizar la llegada de los ordenadores en los hospitales. Allí estuve 24 años. Otra mañana me encontré admirablemente acogido e instalado en un departamento de esta casa con la misión de descubrir y hacer entender, por fin, la bioestadística, a los alumnos de pre y post grado de esta queridísima facultad de medicina y aquí permanecí más de 30 años hasta

mi jubilación". También destacó su cercanía y colaboración con la SEIS, "En medio de tal cúmulo de actividad frenética en 1990 unos cuantos veteranos miembros de la SEIM, contagiados y dirigidos, como no, por Luciano Sáez, entendimos que había llegado la hora de dar un giro a una sociedad en la que tanta esperanza habíamos puesto para ampliar su filosofía, su campo de acción y su desarrollo ante el horizonte imparable de las nuevas tecnologías de la información. Dimos cabida en ella a cuantos profesionales dedicaban su esfuerzo a cualquier rama de la salud y así surgió la SEIS. Esta nueva SEIS otorga ahora un premio a este viejo profesor".

4. Premio Nacional de Informática y Salud 2013, al Trabajo realizado para difundir la implantación de las Tecnologías de la Información y la Comunicación en Salud. Concedido a CSC, por su coordinación y gestión del showroom de innovaciones tecnológicas instalado en INFORSALUD y por la implantación de soluciones TIC de salud en Latinoamérica con más de 2.500 instalaciones distribuidas en esta zona geográfica donde sus soluciones TIC cubren la asistencia sanitaria de más de 62 millones de personas. Entregó el Premio **Juan Fernando Muñoz Montalvo**, subdirector general de Tecnologías del Ministerio de Sanidad, Servicios Sociales e Igualdad. Lo recogió **Antonio Alonso Martín,** director de la Unidad de Negocio de Latinoamérica de CSC Sanidad, que agradeció la presencia de todos los asistentes y, por supuesto, a la SEIS que les otorga el premio. "Como ha dicho Emilio Aced estamos intentando difundir, por toda Latino América un software español, hecho por españoles. Este premio no sería posible sin la ayuda de todos los compañeros de CSC, pero quiero nombrar a una persona de CSC, que siempre está en la sombra y que es de las personas que más han hecho por los sistemas de información y que continuamente trabaja para sacar adelante todo nuestro trabajo. Me refiero a Ángel Torralba que está entre nosotros".

5.- Premio Nacional de Informática y Salud 2013, al esfuerzo institucional o personal de investigación o innovación en proyectos para la utilización de las Tecnologías de la Información y la Comunicación en Salud. Concedido al Centro Nacional para el Desarrollo Tecnológico Industrial (CDTI), ya que lleva más de 36 años financiando la I+D+i empresarial como medio para lograr una economía más competitiva y un mayor bienestar en la sociedad. Su actuación se caracteriza fundamentalmente por su vocación de servicio a la empresa, la oferta de los instrumentos financieros más adecuados y el apoyo en la sistematización de proceso innovador en la empresa. Entregó el Premio **Mª José Marzal,** directora de ComputerWorld y lo recogió **Elisa Robles**, directora general, que, en sus palabras tras



Antonio Alonso recoge el premio de manos de J.Fernando Muñoz.



Elisa Robles recoge el premio de manos de María José Marzal.

recoger el premio, dijo "Para mí es muy grato en mi nombre y en nombre de todo el CDTI, recoger este premio en reconocimiento a la labor del fomento a la innovación. Llevamos más de 36 años apoyando la innovación, esencialmente la innovación de base tecnológica entre las empresas españolas y entre los agentes del sistema de I+D+i, es decir, que estamos en la parte superior del proceso que es donde esta Sociedad SEIS normalmente trabaja. Apoyamos que las empresas desarrollen tecnologías de la información. ¿Y por qué hacemos esto? La respuesta es que se trata de un medio para generar empleo, para generar valor añadido y, en definitiva, para que la sociedad funcione mejor lo cual, en

estos momentos, nos hace mucha falta en España. Agradezco a los organizadores, no solamente porque nos hayan otorgado este premio sino también que hayan otorgado este premio dando tanta importancia a la innovación. Muchas gracias."



Manuel Verdugo recoge el premio de manos de Juan A. Vargas



Luis A. Hernández recoge el premio de manos de Francisco Fernández

6. Premio Nacional de Informática y Salud 2013, a la mejor Aportación presentada en las actividades de la SEIS durante los últimos 12 meses. Concedido a Manuel Verdugo Páez, del Servicio Canario de la Salud, por HIPOT (Herramienta Informática Portátil y Táctil para la Comunicación No Verbal) que es un proyecto de investigación enfermero puesto en marcha en la Gerencia de Servicios Sanitarios del Área de Salud de Lanzarote y que desde el 2014 se ha ampliado al Servicio Canario de Salud y que ha conseguido abrir nuevas vías de comunicación entre pacientes con dificultad en la expresión verbal. Dicho proyecto ha originado la creación de una aplicación para dispositivos móviles basada en Patrones Funcionales de enfermería. Entregó el Premio **Juan Antonio Vargas Núñez,** decano de la Facultad de Medicina de la UAM y lo recogió **Manuel Verdugo Páez,** de la Unidad Técnica Gerencia de Lanzarote, con las siguientes palabras. "Agradezco este premio a la SEIS, al Servicio Canario de Salud y a la Gerencia de Salud de Lanzarote, por el apoyo prestado y especialmente a Javier López Cavero que creyó y apoyó siempre este proyecto y a los compañeros que han trabajado en él. Gracias a todos."

7. Asimismo, se acuerda conceder un Premio Especial de Informática y Salud 2013 a la Consejería de Salud y Política Social del Gobierno de la Junta de Extremadura, por haber impulsado una de las políticas más innovadoras que han convertido a Extremadura en todo un referente nacional en la incorporación de las nuevas tecnologías a todos los procesos de la administración sanitaria. Entregó el premio **Francisco Fernández,** director de Correo Farmacéutico y Diario Médico, y lo recogió **Luís Alfonso Hernández Carrón**, consejero de Salud y Política Social del Gobierno de Extremadura, que se expresó en los siguientes términos: "Es un orgullo para nosotros recoger este premio y quiero compartirlo con los profesionales de Extremadura que están trabajando en el área de tecnología de las TIC en sanidad. Nuestra Comunidad Autónoma apostó, hace ya algunos años, por la implantación de las TIC en sanidad y creo que este premio viene a reconocer esa apuesta que sin duda ninguna no ha cesado y va a seguir porque produce muchas satisfacciones para los pacientes, para el personal sanitario. Esa apuesta quiero compartirla con los presidentes de los Colegios de Farmacia de Cáceres y Badajoz que nos han ayudado a implantar las tecnologías de la información en la Sanidad. También quiero agradecer al Ministerio de Sanidad el que vayamos de la mano en los proyectos que estamos desarrollando en Extremadura y estemos liderando algunos grupos de trabajo que estamos poniendo en marcha y que nos van a permitir seguir mejorando algunos problemas. Muchas gracias a todos. Para nosotros este premio ha sido una inyección de ánimo para seguir trabajando en esta materia. Muchas gracias, de nuevo."

8. Igualmente, se acuerda conceder una Mención Honorífica a Josep Manyach por el impulso e innovación de las Tic en Salud en los diferentes cargos de responsabilidad que ha desarrollado a lo largo de su carrera profesional como, por ejemplo,

presidente del Consorcio Sanitario del Maresme, director de la Fundación TicSalut, y coordinador de la Comisión Departamental para la Coordinación de las TIC del Departamento de Salud de la Generalitat de Cataluña. Entregó la mención honorífica **Mª José Marzal,** directora de ComputerWorld y lo recogió el **prof. Manyach**, que agradeció el galardón con las siguientes palabras: "Gracias por esta mención honorífica que viene a cerrar mi carrera, y un doble agradecimiento. Por un lado a la SEIS por esta capacidad de transformación y de adaptación al sistema sanitario y a este impulso que ha dado a las TIC y, de otro lado, a la propia Consejería de Salud de nuestra Generalidad porque me ha permitido trabajar en un ámbito en el que partiendo de la gestión sanitaria, he entrado en las tecnologías y he visto cómo éstas se han imbricado en los procesos asistenciales y en el trabajo de todos nuestros profesionales de salud.

Y ahora, para hacer una especie de testamento, entiendo que todavía hay un par de retos: uno es integrarnos mucho más, es decir, que la tecnología ya no es problema, la tecnología está muy trabajada y el otro, es que hay que integrar a los ciudadanos en el proceso de salud y también hay un reto más que es el tema de los servicios sociales. Decir salud con el tema de las enfermedades crónicas, del envejecimiento de la población ya no termina propiamente en los servicios asistenciales sino que hay un factor de prevención y un factor de asistencia en el ámbito social en el que las TIC son un instrumento muy importante para que haya esta continuidad asistencial. Espero que la SEIS se integre y se proyecte hacia esta integración de todo el proceso social del sistema de salud mediante las tecnologías."

9. Finalmente, se acuerda conceder una Mención Honorífica al Campus de Excelencia Internacional "AndaluciaTech", por conseguir el primer título de Grado en España sobre Bioinformática e Informática Clínica. Es un título que se imparte de manera conjunta entre las Universidades de Málaga y Sevilla en el marco del campus de excelencia de Andalucía Tech. El grado combina los campos de la Ingeniería Biomédica, la Bioinformática y la Informática Clínica. Entregó la Mención Honorífica Juan **Antonio Vargas Núñez,** decano de la Facultad de Medicina de la UAM y recogió la Mención Honorífica **Ramón González Carvajal**, vicerrector de Transferencia de la Universidad de Sevilla, que agradeció el premio en estos términos: "Agradezco a la SEIS esta mención que para nosotros es muy importante, como universitarios, que se siga reconociendo el papel que desarrollamos al crear el campus "Andalucía Tech". Uno de los temas a los que nos dedicamos estaba vinculado a la salud, por una sociedad saludable y, por otro lado, teníamos especial interés en las comunicaciones. Cuando estudiamos el plan



El profesor Manyach recoge el premio de manos de Mª J. Marzal.



Ramón Gonzalez Carvajal agradeciendo el premio recibido.

tecnológico del campus realmente existía un nicho de formación en el campo de la informática clínica. No se trataba de un nicho, iba a ir a más. Estamos razonablemente contentos pensando en lo que llamamos informática médica, para dar una idea de ser algo multidisciplinario. Estamos muy orgullosos con esta distinción. Muchas gracias."

Entregado este último premio el moderador rogó a los premiados y autoridades que subieran a la tribuna para hacer una foto de familia. Hecha ésta, comenzó el concierto de música de cámara a cargo de **Rafael Domíngue**z (Violonchelo) y **Antonio Palmer** (Piano). A la finalización del mismo se sirvió un Vino Español.

XI Foro de Seguridad y Protección de Datos de Salud

PAMPLONA 19 Y 20 DE FEBRERO DE 2014

Los días 19 y 20 de febrero la SEIS y el Gobierno de Navarra celebraron la XI edición del Foro de Protección de datos de Salud, bajo el lema "Salud 2.0 y mSalud. Seguridad y confidencialidad de la información sanitaria en la sociedad conectada". El acto se celebró, como el año anterior, en el Planetario de Pamplona.

ACTO INAUGURAL



Estuvo presidido por **Juan José Rubio Vela**, gerente del Servicio Navarro de Salud, al que acompañaban **Luciano Sáez**, presidente de la SEIS; **Iñaki Pariente de Prada,** director de la Agencia Vasca de Protección de Datos; **María José Blanco**, secretaria general de la Agencia Española de Protección de Datos y **Ramón Miralles**, coordinador de Auditoría y Seguridad de la Información de la Autoridad Catalana de Protección de Datos.

El Presidente de la mesa dio la palabra, en primer lugar, a **Luciano Sáez**, quien agradeció a las instituciones y personas que intervinieron e hicieron posible la celebración del Foro. Recordó que en el año 2004 la SEIS organizó el Foro de Protección de Datos de Salud con la misión de crear un espacio de encuentro entre el sector tecnológico, autoridades y profesionales que se ocupan del tema central del Foro. Los objetivos que se establecieron fueron:

a) Sensibilizar y concienciar a todos los actores implicados para garantizar una atención sanitaria de calidad y para definir políticas adecuadas para la protección de datos personales e implantar en los sistemas de información las medidas de seguridad que correspondan.
b) Fomentar el establecimiento de canales en los que participen las autoridades de protección de datos para poder llegar a tener un conocimiento directo de las necesidades y peculiaridades del sector sanitario y expresar sus opiniones y recomendaciones en este sector.
c) Potenciar el uso de las TIC para facilitar el cumplimiento de la legislación sobre la protección de datos personales y de las normativas sobre seguridad de la información en el ámbito sanitario.
d) Ayudar en la implantación de medidas de seguridad y soluciones tecnológicas que, aplicadas al sector sanitario, garanticen la calidad del proceso.

Posteriormente, enumeró los foros celebrados hasta este momento así como los lugares en los que tuvieron, hasta que se llegó a un acuerdo de colaboración con el Gobierno de Navarra para constituir en Pamplona la sede del foro, donde nos hemos venido reuniendo desde el año 2007. Como consecuencia de la importancia de la seguridad de la información, se constituyó la Red de Responsa-

bles de Seguridad del Sector Sanitario. Aprovechó para dar la bienvenida a los alumnos de la primera edición del Master de Dirección de Sistemas y Tecnologías de la Información y las Comunicaciones para la Salud, que organiza la SEIS junto con la Escuela Nacional de Sanidad, que están asistiendo a este foro para celebrar su reunión presencial.
En esta XI edición se abordaron los retos y oportunidades que proporcionan las modernas herramientas de interacción social. N mencionó a las empresas que junto con Sodena hacen posible este foro. Iñaqui Pariente de Prada tomó la palabra seguidamente para indicar que 2014 es un año especialmente importante para la Agencia Vasca ya que cumple 10 años desde su creación.

Ramón Miralles intervino para, en primer lugar, excusar la ausencia de la directora de la Agencia Catalana de protección de datos, que en el día de hoy había tenido que presentar la memoria de la Agencia en el Parlamento. Felicitó a la SEIS la organización de esta XI edición y reconoció los esfuerzos que realiza para poder reunir a todos.
"Quiero señalar que el contexto o el paradigma de la sociedad de la información que nos ha tocado vivir es complejo y con muchas variables, de las cuales quiero señalar tres. La primera es que las tecnologías de la información, de una u otra manera, van unidas a las personas. La segunda variable es que todas esas tecnologías que nos preocupan están conectadas por lo que la complejidad aumenta. Hay un tercer elemento que complica más la situación y que obliga a reflexionar más, y es que estamos ante un modelo absolutamente cambiante". Citó cómo anécdota que alguien, en el 2010, dijo que la privacidad había dejado de existir y cuatro años más tarde, la misma persona que no es otra que Mark Zuckerberg, afirmaba que la seguridad era algo vital. "Durante estos dos días vamos a intercambiar experiencias para ver si somos capaces de encontrar soluciones a este tipo de problemas".

En cuarto lugar intervino **María José Blanco** que felicitó a la SEIS y a las autoridades de Navarra por su colaboración y a todos los asistentes. "Aunque llevemos once ediciones, quedan muchas cosas por decir. Estamos ante una revolución tecnológica en la que no tienen tanta relevancia las herramientas para calcular los datos como los datos mismos y el uso que se hace de ellos".

Finalmente y con breves palabras, **Juan José Rubio Vélez** intervino para dar las gracias a la SEIS por elegir, una vez más Pamplona, y por la labor que vienen realizando desde hace varias décadas en beneficio de la salud. Sin más, declaró inaugurado el XI Foro de Seguridad y Protección de Datos de Salud.

PRIMERA SESIÓN

"SOLUCIONES Y HERRAMIENTAS PARA MEJORAR LA SEGURIDAD"



El moderador de esta primera sesión fue **Valentín Elizondo Nevares**, director general de Gobierno Abierto y Nuevas Tecnologías Gobierno de Navarra. Y los participantes fueron:

Mariano J. Benito, CISO (Chief Information Security Officer) de GMV, que habló sobre "Protección de Datos de Salud. ¿Necesidad del Gestor, del usuario o mero requisito legal?"; **Manuel Barrios Paredes**,

responsable de la línea de Auditoría de Seguridad Informática de El Corte Inglés, con la ponencia, "Estrategia de seguridad ante amenazas persistentes avanzadas"; **Luis Pablo del Árbol Pérez**, responsable de Desarrollo Producto con Seguridad de Telefónica Digital España, que trató el tema "Cyber Security in the Digital World"; **Juan Díaz García,** coordinador de la Red de Responsables de seguridad de la Información Sanitaria y responsable de la Unidad de Gestión de Riesgos Digitales Subdirección de Tecnologías de la Información del Servicio Andaluz de Salud. Expuso "El resumen de actividades de la red de responsables de seguridad de la información sanitaria"; **Juan Ramón Fontán Lago**, sales director Security Spain Accenture; **María Gutiérrez Puente,** responsable del Área de Seguridad TI de Fujitsu, que habló sobre "Retos de Seguridad y Confidencialidad en la nube"; **Sofía Moreno Pérez,** del Proyecto FIRE. "Investigación y seguridad TIC en salud para Horizon 2020", y **Carlos Piqueras Picón,** business development manager de Digital Health de Intel Corporation Iberia, S.A.

El primero en tomar la palabra fue **Mariano J. Benito**, que habló acerca de los derechos de los ciudadanos en materia de seguridad y cómo los usuarios tienen actualmente más conocimiento. "La visión que tenemos desde GMV es que la LOPD ha pasado de ser un derecho antes desconocido, a convertirse en un tema propio de las conversaciones de la gente. El volumen de datos que se generan actualmente superan enormemente el de hace 20 años. Si actuamos inteligentemente podemos conseguir que la protección de datos se encuentre embebida dentro de todos nuestros procesos. Si además lo combinamos con un estándar internacional en seguridad de la información y combinado con el conocimiento que tenemos, podemos llegar a conseguir que las cosas en esta materia se hagan solas o las tengamos muy enfocadas".

Seguidamente fue el turno de **Luis Pablo del Árbol Pérez.** Dio su punto de vista sobre cómo securizar y evitar ciberamenzas de todo lo que se genera en torno a las aplicaciones e-health. "La información se encuentra actualmente a solo un clic de distancia y es accesible desde cualquier sitio, y debido a esto hay que tener mucho cuidado con lo que se publica y cómo se protege. El acceso a aplicaciones e-health por parte de los usuarios de forma remota y fuera de los entornos hospitalarios, conlleva nuevos desafíos en materia de fraudes. Si no somos capaces de saber por qué se producen las ciberamenazas y cómo detectar futuros ataques, no vamos a poder solucionarlo ni a poder establecer futuras estrategias de seguridad".

Juan Rámon Fontán Lago dio tres ideas de *accenture* para la protección de la información en el ámbito sanitario. "Las capacidades de detección de ataques todavía no están lo maduras que deberían. Nos preocupa la situación de la percepción que tienen los responsables de seguridad acerca de sus prioridades, quedando plasmado en un estudio realizado que el 58 % afirma no disponer de muchas medidas de seguridad. En el contexto actual donde estamos abriendo la puerta de la información de salud al mundo, la forma de mantener segura la información es mantener un bastión sobre la información cuando todo tiende a encontrarse interconectado favoreciendo el robo de información".

Posteriormente fue el turno de **Manuel Calderón Palacios**. "El sector salud es un sector incluido en el plan nacional de infraestructuras críticas. Desde la tablet que lleva el cirujano hasta el equipo de sobremesa en recepción, son dispositivos con posibilidad de contener malware que se replicará en todos y cada uno de los dispositivos de una instalación sanitaria. Cada día son más los dispositivos que añadimos a nuestro entorno sanitario que disponen de una toma USB y una toma de Red convirtiendo estos dispositivos en una puerta más de entrada para los ataques. Muchas veces los equipos se instalan con perfil de administrador, ya que es más cómodo para poder instalar software, pero también es un peligro potencial para el malware. Los usuarios son el eslabón más débil por lo que se debe llevar a cabo un labor de concienciación".

María Gutiérrez Puente contó una primicia para los asistentes al foro y es que, "desde nuestro punto de vista, la computación en la nube será uno de los entornos más seguros. Dentro del modelo de nube disponemos de muchas ventajas aunque también de riesgos en materia de privacidad. Por ello, como primicia, quiero contarles que nuestros matemáticos han diseñado un modelo, el cifrado homomórfico, que nos permite tratar la información cifrada como si se encontrara sin cifrar, garantizando la privacidad de los datos. Estos mecanismos de cifrado homomórfico se encontrarán disponibles en nuestro servicio en la nube en Europa a lo largo de este año."

Sofía Moreno Pérez presentó los resultados provisionales de un proyecto europeo que se llama FIRE que fundamentalmente se trata de que en hay ins-

titutos y universidades tecnológicas muy brillantes y sin embargo la industria no está a la altura. Horizon 2020, que es el nuevo programa de investigación europeo, intenta realizar un abordaje multidisciplinar de este problema

Finalmente, **Juan Díaz** hizo un resumen sobre la Red que se constituyó hace un año para que todos los que se encargan de temas de seguridad tuvieran una línea de trabajo que permitiera localizar los problemas comunes.

SEGUNDA SESIÓN

"CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN EN ATENCIÓN DOMICILIARIA A LOS ENFERMOS CRÓNICOS"



Iñaqui Pariente de Prada, director de la Agencia Vasca de Protección de datos fue el moderador de esta sesión. Los ponentes fueron: **Guillermo Viñegra García**, viceconsejero del Departamento de Salud del Gobierno Vasco; **Miren Bagües Bafaluy,** de Saludnova S.Coop; **Iñaqui Martín Lesende,** médico de familia y responsable del proyecto TELBIL; **Jordi Martínez Roldán**, director de Innovación de la Fundación TicSalut, y **Mikel Ogueta Lana**, subdirector de Información Sanitaria y Calidad del Servicio Vasco de Salud, Osakidetza.

Comenzó el moderador dando la palabra a **Iñaqui Martín** para que, desde la práctica y desde un proyecto piloto como es TELBIL, comentara cómo se implantaba un proyecto piloto y cómo se llevaba a la práctica y, en definitiva, cuáles eran las expectativas iniciales. Dijo Martín que el proyecto TELBIL surgió casi como una necesidad de incorporarse a las nuevas tecnologías en el ámbito clínico asistencial, con bastantes incertidumbres porque cuando se comenzó no había mucha experiencia como para tener unas directrices claras. "Nos lanzamos a lo que al principio fue un ensayo clínico aunque ahora estamos ya en una fase de implementación y de evaluación. Para ello seleccionamos unos pacientes muy complejos, con patologías como insuficiencia cardíaca y la broncopatía crónica. Ahora también se incluyen enfermos con pluripatología, multiingresadores, con al menos dos ingresos en el último año. Una característica básica es que tenían que ser pacientes domiciliarios

Respecto a cómo admiten los pacientes el uso de la tecnología, el ponente dio dos datos: Uno, es que en la práctica las personas mayores, ayudados a veces por su familia, han recibido bien esta tecnología y son escasos los abandonos. Informó sobre el resultado de una encuesta de satisfacción realizada a los pacientes que seguían tele monitorizados. En los ítems que tenían que ver con la tecnología, en una escala de 5, la media sobre la facilidad de uso fue de 4,8. El mismo valor sobre el poco tiempo que necesitan para enviar sus parámetros, y 4,9 su nivel de satisfacción con estos procedimientos. Fueron 4,96 los que quieren seguir tele monitorizados.

Mikel Ogueta intervino para ofrecer el punto de vista de Osakidetza, y comenzó diciendo que para

ellos es clave la protección de datos. "Todos nuestros proyectos pasan por una fase piloto que están siempre muy controladas y muy limitadas, tanto en el espacio como en el número de pacientes. La idea es que todos los pilotos que hayan tenido éxito se extiendan a toda la población y se convierta en un proyecto corporativo de Osakidetza. Es clave que esa información que se está generando pase a la historia clínica para uso de los asistenciales. La parte asistencial al final es un equilibrio entre la seguridad y la accesibilidad.

Miren Bagües comentó que en todos los proyectos en los que han participado, la parte tecnológica la asumen ellos. "Intentamos que los datos estén protegidos para no violar la ley de Protección de Datos, es decir, nos ocupamos de todos los factores de seguridad. Una vez que los pilotos funcionan, la información se integra. En el proceso de integración lo que hay que intentar es que los datos que están en el hogar lleguen a Osakidetza. Hay que crear túneles seguros por los que llegue la información que está en el hogar a la plataforma y que desde allí llegue la información a Osakidetza. La idea es que en este mundo de la telemedicina hay, primero, una fase de pilotaje y en segundo lugar, la fase de implantación, que es en la que hay que tener en cuenta todo lo relacionado con la ley de protección de datos.

Jordi Martínez intervino para comentar su estrategia que es muy parecida a la de Osakidetza. "Cataluña tiene algunas cosas diferentes ya que por su organización tiene unas 60 estaciones de trabajo clínico diferentes y eso nos obligó a crear la historia clínica compartida, que permitiera compartir la información. Esa historia clínica nos impone trabajar con los entornos de interoperabilidad y estandarización de las comunicaciones y de hecho, esta historia clínica compartida está evolucionando para poder intercambiar datos. Tenemos proyectos en los que los pacientes disponen de una Tablet, proporcionada por Telefónica, por Vodafone o por quién sea, y con los que también se usa bluetooth. Hay otros proyectos en los que transmitimos directamente sobre CAP porque el primer aviso que nos dan los clínicos es que la gente quiere trabajar con una única estación de trabajo. No quieren estar entrando y saliendo y al final, por detrás, los técnicos son los que tienen que hacer transparente toda la información. También tenemos proyectos no presenciales que permiten hablar de profesional a profesional, relación profesional con paciente y relación paciente con paciente.También tenemos experiencias con oficinas de farmacia en las que el dato viaja directo. La primera cosa que debemos tener en cuenta es el tema de interoperabilidad porque los actores, en nuestro caso son varios, y porque además ahora estamos trabajando para integrar la parte social, cosa que es muy difícil sobre todo por el tema de seguridad, desde el punto de vista legal. Desde el hospital, por ejemplo, y gracias a resolver los problemas de interoperabilidad, se puede acceder a información de primaria con independencia del proveedor".

Guillermo Viñegra ofreció el punto de vista del ejecutivo de temas de gestión. Comentó que hacía poco tiempo estuvo en un foro de gestores de sistemas de salud y se dijo que las nuevas tecnologías eran la gran esperanza para la sostenibilidad del sistema. Añadió que los sistemas nacionales de salud están muy presionados porque, en primer lugar, falta dinero. "Nuestro sistema vasco de salud, como el navarro, está en esa situación. También influye el aumento de la esperanza de vida, tanto en hombres como en mujeres. Según el Instituto Vasco de Estadística, en el año 2020 el 25% de la población vasca tendrá más de 65 años. Si además la entrada de población es escasa y el crecimiento vegetativo en el momento actual es negativo, nos encontramos con unos problemas que los diferentes sistemas de salud tenemos que afrontar. Sobre la mesa se han puesto herramientas cortas de efectos rápidos y económicos. Los funcionarios saben que en los últimos 5 años no han subido los sueldos y que los ingresos se han visto mermados por varios motivos más. Tenemos que abordar la prestación asistencial de otra manera. La línea estratégica que se está ahora implantando en el país vasco y nuestro Plan de Salud que acaba de aprobarse para el 2013-2020, es una línea que cubre la vejez, la cronicidad y la dependencia y digo primero vejez porque ella nos lleva a la cronicidad de la cual se pasará a la dependencia".
Hay que añadir que "los nuevos roles que estamos queriendo poner a la enfermería de atención primaria viene sostenida con una historia clínica para ellas que se llama Osanaya. Otro de los temas en los que hay que interactuar es que las personas tienen que ser responsables de su propia salud. Un diabético tiene que conocer la vigilancia de su enfermedad y su tratamiento".

Iñaqui Martín comentó que tomaron unas medidas que han sido aceptadas para elaborar un con-

sentimiento informado, pero no al uso. Tuvimos en cuenta, en el terreno en el que nos estábamos moviendo, un sistema que ya explicábamos por escrito, con doble firma, dónde quedaba claro dónde iban los datos que ellos manejaban y quién iba a acceder a estos datos (los coordinadores del estudio y también la empresa). En la encuesta que se hizo, la confianza que se tenía antes en estos comentarios era de 4.9 sobre 5, es decir, que por parte de los pacientes que fueran a participar había una total confianza. Dejábamos bien claro la confidencialidad de los datos y la codificación de los nombres para que no faltara la confidencialidad. Desde el punto de vista tecnológico algo que también firmamos y dejamos muy claro es que esto es una ayuda.

Mikel Ogueta dijo, sobre los consentimientos informados, que lo primero que hay que tener claro es que la monitorización es una operación, es decir, que es una opción en la que hay una alternativa y un complemento a la forma de trabajar y de asistir al paciente que se acepta. La aceptación de los pacientes suele ser muy elevada ya que el enfermo lo que quiere es estar en casa si puede evitar las molestias de tener que acudir a un centro. Los consentimientos informados tienen que estar adaptados a lo que se vaya a hacer.

El moderador se interesó por los aspectos jurídicos del responsable de los ficheros, si hay terceros que intervengan además de la empresa que gestiona la plataforma y si se definieron jurídicamente estas cuestiones. **Miren Bagües** comentó que el dueño del fichero es la empresa, que en este caso Osakidetza, no son ellos los propietarios de la información sino solo la empresa que da el servicio. Nosotros somos los responsables de cumplir todo lo que dice la ley sobre protección de datos para salvaguardarlos. En términos de medidas de seguridad, como la empresa no tiene las medidas necesarias para poder cumplir con la ley, lo que se ha hecho es subcontratar a otra empresa para que salvaguarde estos datos.

Sobre este tema **Jordi Martínez** comentó que en Cataluña, cada proveedor con su sistema es el garante de que se cumpla todo lo relacionado con la ley.

TERCERA SESIÓN

CASOS PRÁCTICOS



Estuvo dedicada a comentar por parte de las autoridades de protección de datos los casos prácticos más interesantes ocurridos durante el último año. Moderó la sesión **Pedro Alberto González**, responsable del Registro de Ficheros y nuevas tecnologías de la Agencia Vasca de Protección de Datos.

Comenzó **Emilio Aced** con un caso de Navarra que es curioso y poco habitual. Se trata de una denuncia que llegó a la Agencia y que afectaba al Departamento de Educación de Navarra ya que una profesora tuvo una falta de asistencia al trabajo y existe un Decreto Foral que ordena publicar, para uso del profesorado, una lista con las ausencias y el motivo correspondiente. Y este era el problema. El motivo de la ausencia se manifestaba por un código, cuya lista se podía consultar por la intranet. Cualquier profesor conoce el significado de todos los códigos. Esta seño-

ra pidió permiso para "técnicas de fecundación", por lo que, todos los compañeros de trabajo supieron que había ido al médico y el motivo. El Gobierno de Navarra alegó que había un decreto foral que obligaba a hacer las cosas de esta manera. La Agencia lo aceptó pero le parecía excesivo que en este listado se publicara el motivo de la ausencia. Aceptaban que la dirección del centro conociera la causa de la falta, pero no que estuviera al alcance de todos los compañeros. Durante la tramitación del procedimiento el propio Gobierno de Navarra tomó medidas y siguió manteniendo la obligación de publicar estas listas, pero suprimió el código o el motivo por el cual se producía la ausencia".

A continuación **Carles San José** habló sobre una denuncia poco habitual, porque ocupaba más de 200 páginas, por lo cual nos preocupamos un poco. Se trababa del empleado de un centro que se dedicaba a tratar datos sobre pacientes con sida y que le remitían desde varios hospitales de Cataluña. Esos datos se enviaban para hacer una estadística relacionada con la patología y se manejaban sin consentimiento de los pacientes. Es verdad que esa estadística estaba declarada de interés por la Generalitat y por tanto había un cierto amparo para realizarla. La Agencia Catalana consideró que para hacer esa estadística no era necesario que los datos de los pacientes estuvieran asociados a su identidad. Al ser el sida una enfermedad de declaración obligatoria, los hospitales tenían la obligación de declarar los datos previstos en estos casos para enviar al centro del estudio. Hasta ese momento todo era lícito, pero el problema fue que algunos hospitales enviaban más datos de los necesarios. El centro alegó que eran los datos de declaración obligatoria, pero era muy sencillo desvirtuar esos datos en el sentido de que no todos los hospitales mandaban los mismos. El tema del caso es que la persona denunciante, que estuvo empleada en ese centro, aportó datos que extrajo de su lugar de trabajo, es decir, documentación e información a la que tuvo acceso como empleado en su momento y que luego la acompañó en la denuncia. La polémica del tema es que hay gente que discute que realmente la autoridad deba tener en cuenta pruebas de este estilo, es decir, obtenidas de espaldas al empleador. Puede darse una cierta deslealtad pero se consideró que el uso que le daba esa persona es ponerla a disposición de la autoridad competente para que, a quien corresponda, decida si el tratamiento es lícito o no. Le dimos validez a esa documentación y ello no impidió que se llevaran a cabo las investigaciones y posterior procedimiento.

Continuó con otro caso. Una persona se quejaba de haber facilitado datos personales suyos y no haber recibido la información que establece el artículo 5 de la LOPD. Era una persona que quería acceder a los datos de la historia clínica de su madre, ya fallecida hacía muy pocos días y en una situación que a la familia le indujo a pensar que se trataba de un caso de mala praxis. Por eso la hija solicitó la historia clínica. El hospital tenía un formulario para pedir la historia clínica en la que se recogían los datos de la persona solicitante, además del titular de la historia clínica. En ese formulario debería constar la cláusula informativa que debía haber en todo formulario de recogida de datos. Es un caso cada vez más frecuente pero todavía hay algunos lugares en los que no existen esos formularios. En principio, el derecho a la información, es decir, toda esa información que hay que dar cuando se recogen los datos, como en qué fichero se incorporan, para qué finalidad, quién es el responsable, ante quién se puede ejercer el derecho, etc., en principio, para esos documentos, hay libertad de forma pero cuando se recogen los datos a través de un formulario, como en este caso, debe figurar, según la ley, expresamente esa información, que en el caso que nos ocupa no había.
La controversia de este caso es que se generaron dudas ya que la persona que facilita los datos, muchas veces está pidiendo el acceso a su información, es decir, vendría a ser como un derecho de acceso la LOPD. Entonces, se genera la duda de si en casos de ejercicios de derechos arco, es decir, el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales, si debe también incluirse en la cláusula informativa y la razón de la duda es que quien ejerce el derecho arco, previamente ya habrá facilitado los datos al responsable del fichero. Es verdad que sucede muchísimas veces que cuando vas a pedir el acceso a la historia clínica, o a la rectificación o cancelación, el hospital ya tiene tus datos y ya le habrá informado en teoría, previamente. De ahí la duda en la controversia. Pero claro, ninguna duda hay en los casos en los que quien ejerce el derecho no es la persona de la que ya se tenían los datos, sino un familiar como en lo que comentamos. Entonces entendemos que ante la posibilidad de ese derecho lo ejerza alguien distinto al paciente, es mejor tener la cláusula informativa porque sino en esos casos no se habrá informado. Pero además, la finalidad inicial, por la que se recogen los datos para la asistencia médica, es una y cuando se recoge la información para hacer efectivo el derecho al acceso a la historia clínica, la finalidad es otra. En este caso la finalidad es gestionar la petición y dar la

historia clínica con lo cual entendemos que en ese tipo de formularios debe figurar la cláusula informativa y en el caso que tratamos, no estaba.

Juana Mª Vegas habló del deber del secreto. Advirtió que en materia de datos sanitarios, la Agencia Vasca no tiene un gran volumen de trabajo, quizás porque en Osakidetza hay un espíritu de colaboración y ayuda con respecto a nosotros y en cuanto tienen una duda nos llaman. Existen muy buenas relaciones. "El caso que quiero exponer trata de una enfermera responsable de un servicio de atención primaria de un ambulatorio que tiene problemas y obtiene la baja durante bastante tiempo. Existían una serie de relaciones, no demasiado buenas, con determinado personal del centro y daba la casualidad que en el mismo centro donde ella trabajaba era el lugar donde ella residía. Es decir, aparte de darle la baja vivía allí y le correspondía ese centro. Pasa un tiempo y esa persona pide el alta y descubre que en su historia clínica ha entrado más gente que la que debería haber entrado. Nos pide la tutela ya que ella intuye que hay accesos indebidos. Decimos que no podemos efectuar la tutela hasta que no haya previamente solicitado su acceso al órgano correspondiente, que en este caso era Osakidetza. Lo pide, le dan el acceso y comprueba que hay accesos sospechosos. Primero, la situación de la mujer no era auténticamente correcta, no estaba todavía curada pero ve que hay muchos accesos de mucha gente y no se da cuenta que efectivamente hay muchos de ellos son debidos a la asistencia sanitaria a su persona, tanto de enfermería como de médico e igualmente hay administrativos que supuestamente han entrado en su historia clínica pero para elaborar sus partes de baja. Accesos estos que estaban debidamente cumplimentados y eran debidos, pero detecta que de dos ambulatorios ha habido accesos que no tenían por qué haberse producido ya que ella jamás había acudido a ellos. Puesta la denuncia se tramita y se detecta que efectivamente se han producido accesos indebidos. Uno porque un supuesto jefe de personal quiere saber si esa persona se va a integrar o no. La historia clínica no tiene como finalidad saber si esa persona estaba o no trabajando. El otro acceso lo hizo una persona que quería saber datos sobre su amiga. Se abrió un expediente, se comprobó que se trataba de una infracción grave y se llevó al contencioso. Esa persona alegó que se habían producido más excesos pero la sentencia decidió que este acceso era debido a un cotilleo".

Emilio Aced presentó otro caso y lo hizo con intención de ilustrar a los asistentes con cosas que no deben pasar. "Se trata de un centro de salud de un pueblo grande en el que la enfermería, diariamente, exponía la lista de personas que estaban citadas, lo cual, hasta cierto punto podría ser permisible, pero es que, además, al lado de cada nombre figuraba el motivo de la visita. Una serie de personas que consideraron que esa información no tendría que darse, lo pusieron en conocimiento de la Agencia que comprobó que esos listados estaban violando la confidencialidad de aquellos pacientes, máximo cuando el sistema disponía de una serie de listados en los que no figuraban el motivo de la visita. La Agencia lo declaró como una infracción y dio órdenes al centro para que esto no volviera a suceder".

Juana Mª Vegas expuso este caso: "Se trata de una persona que trabaja en un centro de salud y está de baja. Va a su centro y tiene prisa porque su hijo está enfermo y quiere volver a su casa cuanto antes. Se mete en la consulta y hace que la médico la atienda media hora antes de que le llegara el turno. El médico la atiende, le da el certificado del médico psiquiatra para que ella lo guardara, pero lo principal es que ella acude para conseguir su parte de baja. Hay una amable charla entre la médico y la paciente y este le entrega, por error, el parte de baja de otro paciente y el suyo se queda en la mesa del médico. Al día siguiente acude a la misma consulta un hermano de la persona que se había llevado una baja que no era la suya. La doctora le pide que se lo lleve a su hermana. El hermano se interesa por la salud de su familiar, ya que ignoraba que estuviera en tratamiento médico y la doctora le cuenta que está regular, que tiene algunos problemas, etc,. Situación esta que la protagonista del caso mantenía en secreto incluso con su propia familia. Como consecuencia de ello se montó en todo el pueblo un lio considerable terminando la doctora denunciada por no haber obrado con mas cuidado".

Emilio Aced comentó que había un grupo de casos que se podrían agrupar, como dijo Juana, en un epígrafe llamado Despechos y Resentimientos. "El ser humano, a veces, utiliza cualquier medio que esté a su alcance para molestar".
Citó dos casos. El primero muy sencillo. "En un centro de adelgazamiento y después de una prueba previa al tratamiento, se entrega a la clienta un informe con los parámetros de su estado actual pero hay una confusión por parte de la secretaría del centro y se entrega a dos personas el informe equivocado, es decir, se pone en manos de terceros información sensible. El otro caso, también sencillo, es algo más complicado: Una señora acude a su

centro para pedir hora para determinada consulta para su hijo. La secretaria le entrega los papeles que salen por la impresora y la señora se da cuenta que el nombre que figura no es el de su hijo. Pide que le den los papeles correctos pero la secretaria, después de muchas insistencias, se aferra a decir que no importa, que su hijo vaya a la consulta que le atenderán. Acude a la consulta y allí se encuentra con el titular de su citación. Se denuncia a la Agencia que declara que se ha cometido una infracción".

Con respecto al derecho al acceso **Pedro Alberto** recordó que **Emilio Aced** tenía un caso que quiere que comente. Se trata de un caso sobre el derecho de acceso. "De accesos a historias clínicas hay muchos casos sobre todo en caso de fallecimiento de familiares. La ley admite estos accesos con una excepción que es cuando el titular de la historia clínica hubiera prohibido el acceso a determinada persona. En el caso al que me refiero, un hijo solicitó datos del padre fallecido pero le fueron denegados porque había un documento del padre prohibiendo que su hijo pudiera acceder a sus datos. El hijo acudió a la AEPD que solicitó ver la historia y se comprobó que el hospital había actuado de forma correcta". "Otro caso complicado es el de una Mutua de accidentes de trabajo y enfermedades laborales que recibe una demanda de incapacidad permanente de una persona. La mutua realiza un reconocimiento médico y a la vista del informe deniega la incapacidad al solicitante. Éste pide el informe para recurrir. La Mutua se ampara en la jurisprudencia existente, un caso en el que el Tribunal Supremo negó a una persona el acceso a un informe del especialista que quería ver, después del accidente de tráfico que había sufrido, los varemos que había utilizado el especialista de la Mutua. En aquel caso el Tribunal dijo que no existía derecho al acceso ya que se trataba de una elaboración de un profesional. El interesado recurrió ante la AEPD y la mutua puso encima de la mesa el informe del Tribunal Supremo para decir que se trataba de un informe pericial y como tal ellos entendían que por aplicación de esta sentencia no le amparaba el derecho de acceso. La Agencia lo que vino a decir es que esa sentencia era propia para un tipo de informe en concreto, que se trataba de una actuación pericial y que no le amparaba el derecho de acceso, pero que en este caso era el informe de un médico que había aportado datos proporcionados por el demandante y que si era realmente una historia clínica a la que podía acceder el demandante".

Juana Mª Vegas presentó otro caso relativo a un hijo que pedía acceso a la historia clínica de su madre fallecida. Osakidetza duda en concedérselo o no, pero según la ley, aunque se trate de una persona desheredada, como en este caso, hay que concederle el acceso y solo puede negarse por el deseo expreso del fallecido negando el acceso a sus datos a una determinada persona, como se dijo antes, que no era este caso.

CUARTA SESIÓN

RIESGOS DE LA UTILIZACIÓN DE LOS DISPOSITIVOS Y APLICACIONES MÓVILES



Moderada por **Ramón Miralles López,** estuvo dedicada a revisar los posibles riesgos específicos derivados de la utilización de los dispositivos y aplicaciones móviles en el ámbito sanitario.

Intervinieron **Toni Felguera**, responsable del Área de R+D+i Seguridad de Barcelona Digital; **Manuel García García**, de CESICAT y responsable de Seguridad de la información del Departamento de Salud de la Generalidad de Cataluña; **Manuel López Alcazar,** de Regional Market Access, Emminens Healthcare Services; **Francesc Moya Olvera,** responsable del Área Técnica de la Fundación TicSalut, y **Ángeles Calvet Candela**, responsable de Movilidad del Hospital Germans Trias i Pujol.

Para empezar la sesión **Ramón Miralles,** de acuerdo con el guión establecido, dio la palabra, en primer lugar a **Toni Felguera,** al que pidió que enumerase los principales riesgos que existen fundamentalmente en el entorno de la salud y cuáles de esos riesgos son los primeros que debemos tener en cuenta y cómo se han de gestionar o tratar con el objetivo de minimizarlos o eliminarlos. Comentó que existía una tendencia a compartimentar la vida, la familia, el trabajo y la vida social, pero se estaba viendo que las fronteras entre esos compartimentos estaban desapareciendo ya sea con el móvil corporativo o el personal. "Usamos Linkedin, buscamos gente a través de una red social, de manera que podemos decir que el móvil es nuestro representante en el mundo digital. A través de esta ventana nos movemos, no únicamente en el ambiente profesional sino que también ejercemos funciones ajenas a lo profesional como pueden ser nuestras relaciones personales. Esa mezcla de cosas comporta el riesgo fundamental y es que no existen barreras entre unos y otros fines y que cuando gestionamos la información en realidad se está gestionando nuestra propia vida". Con fines didácticos clasifica los riesgos en diferentes grupos. El principal riesgo es el manejo que hace el usuario de su propia información y el impacto que tiene su propia vida social en internet, sobre la información que maneja, más allá de pasar o no contraseñas. Hay que ser conscientes de que hay un ecosistema dentro del mundo de las apps que no nos favorece para nada. Podríamos preguntarnos cómo se sustentan las apps. Se sustentan de una forma favorable. ¿Se puede realmente vivir de las apps que todo el mundo descarga y utiliza? Los millones de apps gratuitas ¿lo son porque las empresas son altruistas? El mundo de la seguridad, el mundo del cibercrimen tiene muy en cuenta que su foco va a ser el móvil".

Se dirigió a **Francesc Moya** recordándole también la encuesta que hicieron a final del pasado año sobre cómo están las TIC a nivel de centros de salud. En esa encuesta encuentra datos que le llaman la atención. "Decís que, al menos, un 11% de dispositivos que se usan diariamente eran dispositivos móviles y además que el 70% de hospitales y equipos de atención primaria disponían de herramientas de movilidad. Y mi pregunta trata sobre ¿cómo pensáis que está empezando la implantación de este uso?".

Francesc Moya comenzó diciendo que "en Cataluña hay muchos proveedores, cada uno de los cuales tiene sus propios sistemas de información por lo que nos podemos encontrar con un conjunto de 140 centros y unas 60 soluciones. Cuando desde el departamento de salud nos piden información de cómo está el sector o desde el mismo departamento inciden en ir por una línea a nivel de tecnología, la única manera que tuvimos hace 7 años de tener información de los centros, de por dónde están trabajando y como están utilizando la tecnología fue hacer una encuesta que nosotros llamamos mapa de tendencias, para conocer el sector. Los cios de los centros ofrecieron algunos datos de interés. Cuando estaba en saber cuales de estos dispositivos son de movilidad la respuesta fue que un 11% de esos dispositivos eran móviles. Estamos hablando de portátiles y tablets y en este último año el incremento casi se había doblado por el uso de los iPads. Hemos comprobado que en los últimos años se ha pasado de un 10% a un 11% o sea que la penetración de la movilidad dentro de los centros asistenciales no representa un gran incremento. Solo ha crecido el 1%".
Con respecto al tema de los smartphones, "institucionalmente la compra de estos dispositivos para los asistenciales no experimenta ningún incremento. Hay muy pocos y habitualmente son para las capas directivas. Cuando preguntamos sobre la movilidad, para que son utilizados, un 60% contestaban que ya permiten a los portátiles el acceso a la historia clínica. De estos un 32% se referían a las tablets, mientras que los smartphones bajaban a un 18%. En cuanto a los pacientes su uso es masivo y cuando se pregunta qué servicio se le está dando un 25% de esos centros contestan que les dejan acceder dentro del recinto asistencial a internet. También se hacen recordatorios de citas por sms. Un 5% han dado un paso más y están informando sobre resultados clínicos. Solo un centro ha dicho que ellos están utilizando apps de terceros o tienen una propia y ya están prescribiendo. Esta sería la situación a nivel de Cataluña".

Llegó el turno de **Manel Garcia,** al que el mode-

rador pidió que informase sobre qué proyectos o servicios están desarrollando estratégicamente.
Informó de la parte corporativa, de la parte central, lo que es la propia Consejería, y lo que es CatSalut. "Al ser la salud un tema universal, prácticamente nos dirigimos a todos los ciudadanos. Tenemos una web que es el canal Salud donde hay una información sobre temas médicos y esto vale tanto para Pcs como para telefonía. Luego hay servicios más avanzados en los que se da información concreta del paciente que haga una consulta. Desde hace muchos años el Departamento de Salud está avanzando en dotar al sistema de salud de toda Cataluña de unos elementos para compartir información. Por ejemplo la historia clínica compartida, la receta electrónica. Complementando esto lo que hemos hecho es un visor, que es la carpeta personal de salud, que permite que esos mismos datos sean visualizados por el paciente. Este sistema se puso en marcha en el 2009 y lo hemos ido abriend a colectivos mayores. Todavía no está operativo al 100% porque aun hay muchos retos que afrontar. El primer factor que frena su amplia utilización o que desde la Generalidad se haya hecho por disparar su uso intensivo es, principalmente, la forma de acceder. Al ser datos de pacientes concretos y de nivel alto, era necesaria una autentificación fuerte y de momento la tenemos con certificados digitales. El hecho de estar certificados, automáticamente hace que los menores de edad no puedan acceder a estos servicios. Además, todos los sistemas que comento de compartición de información no pasaron del 0 al 100%, sino que cada vez más centros comparten la información y estamos llegando a un proceso de madurez. Ya tenemos un porcentaje muy alto de historias clínicas, de diagnósticos que se comparten. La receta electrónica está prácticamente extendida".

El moderador se dirigió seguidamente a **Ángeles Calvet** para que hablase sobre cómo se están planteando el uso de los dispositivos móviles, tanto desde el punto de vista de los profesionales como de los usuarios. Comentó Angels que "hace prácticamente un año que comenzaron con la idea de desarrollar aplicaciones para móviles tomando esto, al principio como un juego. No teníamos en cuenta nada de seguridad y queríamos sólo crear un prototipo y ver qué hacíamos después. Hicimos solo un directorio de cómo acceder a las redes sociales que tenemos en nuestra zona. Una vez hecho vimos que tenía una gran aceptación entre los asistenciales y el público en general. Como consecuencia de aquello mucha gente nos propuso que hiciéramos una aplicación que aconsejara sobre temas de salud. Paralelamente, como consecuencia de la aplicación que estábamos desarrollando y debido a las sugerencias y peticiones que recibimos, pensamos hacer algo más importante. Desarrollamos una app, teniendo ya en cuenta las medidas de seguridad, que permitía que se pudiera localizar a un paciente y decirle, en caso de una urgencia, los centros de salud más próximos a su localización a los que poder dirigirse. Podía localizar centros de primaria o centros de atención urgente. Se le manda la dirección, el horario y la ruta. En los hospitales se enteraron de lo que hacíamos y a partir de aquí nos comentaron que ellos tenían pacientes que aunque están en su domicilio tienen que consultar muchas cosas al hospital. También nos pidieron una aplicación para control de VIH. Ahora estamos en un momento difícil en cuanto a seguridad. Ahora nos viene todo el mundo con ideas para poder compartir cosas".

El moderador se dirigió a **Manuel López** y le pidió que explicase cómo abordaban el diseño de esos productos, cómo tienen en cuenta la seguridad y también de eficiencia y disponibilidad de los propios servicios, ya que ahora no hablamos solo de confidencialidad y de funcionamiento y que realmente la prestación derivada de este tipo de servicios se mantenga. En definitiva, ¿cómo abordáis el diseño de los productos?, y cómo tenéis en cuenta eso de lo que estamos hablando como privacidad, seguridad, etc. Contestó diciendo que "Emminens provee de una solución destinada a pacientes crónicos, diabéticos por ejemplo, con lo cual tienen un nivel de interactuación con los sistemas sanitarios muy habitual porque continuamente tienen que recibir las pautas de sus medicinas, tienen que modificar en algunos casos la terapia que están siguiendo, tienen que hacer formación, con lo cual tienen una interacción muy habitual. A la hora de diseñar herramientas destinadas a estos pacientes que, en la mayoría de los casos van a hacer sus mediciones, no en el ámbito hospitalario, sino en su casa y mediante una conexión de los dispositivos se va a compartir la información lo cual es muy importante para la toma de decisiones. En el diseño de la plataforma de las soluciones que nosotros tenemos, planteamos dos aspectos fundamentales. El primero, que son herramientas de comunicación, tanto de pacientes a pacientes, de paciente a profesional y de profesional a profesional, como sucede en el caso de las interconsultas".
El moderador le pidió que se imaginase que es un usuario y que se sitúe en el mundo de las apps y cuente de qué manera se puede transmitir al usuario un cierto nivel de confianza. Manuel López contestó diciendo

que "había leído un artículo de Guardiola que había hecho un estudio sobre una empresa y había detectado algunas aplicaciones que están dentro del ámbito de la sanidad que está en los markets de cualquier empresa y hablaba de una aplicación llamada acné que emitía una luz, y que si se encendía diariamente durante dos minutos, según los proveedores, eliminaba las bacterias que se pudieran tener en la cara. La aplicación costaba 2 $ y tuvo 20.000 descargas por lo que podemos calcular fácilmente los beneficios del desarrollador y del propio market que se queda con parte de los beneficios. No hay detrás unos profesionales que puedan avalar esa aplicación. Desde el punto de vista del usuario habrá personas que no caigan en el engaño pero hubo 20.000 personas que se lo creyeron o simplemente quisieron probarlo. Hay 23.500 aplicaciones médicas en el marketplace de Apple. Si la previsión para este es la de 1.700.000 smartphones son muchas las personas que se descargarán aplicaciones médicas. Lo que hay que hacer, como usuario, es fomentar mecanismos que estén avalados por algún organismo, por algún hospital o por una institución que tenga un peso asistencial y que tenga criterio. En la Junta de Andalucía se ha implementado un proyecto que se llama App Saludable y lo que hacen es facilitar un distintivo que es voluntario y gratuito".

Para **Manuel López,** internet es como la calle, y los mercados de aplicaciones son como las tiendas. "Cuando por la calle te ofrecen algo que cura todo, tu ya sabes que esto no es muy fiable. La gente cuando enferma sabe que tiene que acudir a su médico que le pondrá un tratamiento, luego tendrá que ir a la farmacia, al fisioterapeuta, etc. Este sentido común no lo tenemos que perder aunque hablemos de TIC. Y hay que saber que un Smartphone es una herramienta muy poderosa que llevas en el bolsillo y que te abre una ventana a los sistemas informáticos y que tiene un montón de herramientas (linterna, por ejemplo) y también es una tienda que el fabricante de estos dispositivos me pone en el bolsillo con el propósito de venderme cosas".

QUINTA SESIÓN

NUEVOS ENTORNOS DE INTERCAMBIO DE INFORMACIÓN DE SALUD



Estuvo de dedicada a los nuevos entornos de intercambio de información de salud como blogs, redes sociales o grupos de apoyo de pacientes. La sesión fue coordinada por **María José Blanco Antón** y participaron: **Antonio Delgado Planas,** de Forumclinic, profesor de Esade; **Pedro Martín Pérez,** médico de atención primaria del Servicio Canario de Salud; **Roberto Nuño Solinis**, director de O+Berri, Instituto Vasco de Innovación Sanitaria, y **Rosario Serrano Agudo**, directora gerente del Área de Salud de Unidad Editorial. Comentó la moderadora que, en primer lugar, los participantes harían una presentación rápida de sus proyectos para posteriormente informar de cuáles son los puntos fuertes y débiles de cada proyecto y las medidas que han adoptado para garantizar los derechos de privacidad y seguridad y esperando que también nos den información sobre el nivel de confianza de los pacientes o usuarios de estos sistemas y el nivel de implantación de cada uno de ellos.

Dio la palabra, en primer lugar, a **Antonio Delgado** que informó sobre el proyecto Forumclinic. "Este proyecto nace en el 2007 y en el seno del Hospital

Clínico de Barcelona, donde se atiende a los pacientes de forma muy humana y de forma correctísima. Pero por mucha humanidad que haya, después del ingreso el paciente se va a su casa con su o sus enfermedades crónicas donde tiene dudas, angustias y le falta información. Busca entonces, la enfermedad en Google y cree que se va a morir. Para evitar la falta de información por un lado, y la falta de apoyo por otro, se crea la iniciativa de Forumclinic. Se pone así en marcha una iniciativa que elige algunas enfermedades crónicas y da, sobre ellas, una información veraz, para que el paciente se sienta seguro y tranquilo. Por otra parte se busca que los pacientes se pongan en contacto entre ellos y que compartan sus vivencias para evitar la impresión de algunos enfermos con cronicidad que en su casa o con sus amigos se encuentran desatendidos. Con esta plataforma se intenta que se pongan en contacto los pacientes y obtener comprensión y consejos. No se hace teleasistencia ni diagnósticos. Eso lo hace el hospital. Lo primero que se hace es un documental muy divulgativo aprovechando los recursos del hospital. Seguidamente se crea un foro. Se han creado hasta 12. Desde esquizofrenia hasta diabetes, pasando por el cáncer de mama, artritis y artrosis y lo que se hace es informar de cómo es la enfermedad donde hay un experto del hospital que se dedica a moderar ese foro, informando sobre enfermedades escribiendo noticias, etc. El profesional va a ir observando qué pasa en los foros. Cada usuario que se registre en alguno de los 12 foros que tenemos, ya que atendemos 12 enfermedades, puede abrir un chat con el tema que más le preocupe. El resultado ha sido sorprendente ya que hay casi 10.000 usuarios registrados. Los foros son abiertos pero para poder participar hay que registrarse. Al día recibe 7000 visitas y está funcionando muy bien en ese sentido".

A continuación intervino **Pedro Martín**, médico de familia al que se le ha pedido que informe sobre su actividad diaria que, según dice es de 24/7. Lleva cinco años en su centro de salud, con un horario siempre de mañana excepto cuando se hacen guardias de 24 horas. Por ello muchos enfermos le pidieron poder consultarle cosas fuera de su horario, por WhatsApp o por Facebook y les dijo que no tenía ningún problema. A través de esos medios de comunicación se ha establecido contacto con algunos pacientes que no pueden acudir con frecuencia a la consulta. Realmente esto surgió con motivos de algunos pacientes terminales que necesitaban ayuda. Como puntos débiles debo decir que no son entornos fiables para una protección de datos.

Es el turno de **Roberto Nuño,** que habló de Kronikoen Sarea que es una red social dirigida a pacientes crónicos así como a sus cuidadores y a su entorno familiar que se puso en marcha en el año 2012 con financiación del Gobierno Vasco a través del proyecto Agenda Digital e impulsada por el entonces Departamento de Sanidad y Consumo del Gobierno Vasco quien se ocupó de la primera fase de diseño y puesta en marcha. De la dinamización del proyecto se encargó Innovas. En la fase actual Kronikoen Sarea está dentro de la responsabilidad de BioEd (Fundación Vasca de innovación e investigación sanitarias) y dentro de ésta, está el Instituto Vasco de innovación sanitaria.

Rosario Serrano habló de Ippok, que es una red social para el médico y el farmacéutico y pertenece al grupo de Unidad Editorial. "Nuestras experiencias en 2.0 son realmente gratificantes ya que nos permiten estar muy cerca del usuario, conectar con el, interactuar y saber su opinión. Ippok representa un paso más en las tecnologías que están en el mercado y ese paso lo queremos dar de la mano de diario médico.com y de correofarmaceutico.com. Ippok nace a mediados del 2012 y su cuestionamiento social iba a ser una red social solo para médicos. Es cierto que el acercamiento entre los profesionales que lo hemos conseguido muchas veces en nuestras publicaciones y el concepto multidisciplinar hay que llevarlo también a las nuevas tecnologías y nos planteamos la oportunidad, ahora mismo, de experimentar al 100% la unión de los profesionales. Así Ippok nació con el objetivo de ser la primera red social de profesionales sanitarios de habla hispana. Es cierto que hay muchas redes, pero no hay ninguna como esta que aglutine a todos los perfiles. Desde los inicios esa era la vocación de la red. Como red social tiene sus matices ya que en nuestras publicaciones, Diario Médico y correo farmacéutico. com estamos obligados a acreditar que todos los profesionales que nos leen son médicos y farmacéuticos y por ello nuestros registros son cerrados a petición de los profesionales que usan la red, que sea cerrada y que sea vertical para garantizar la seguridad de sus contenidos. Debido a esto, lo primero que hacemos es emular el registro que tenemos ya del diario médico y del correo farmacéutico que nos garantizan que las personas que nos leen son del entorno sanitario, pero en Ippok somos algo más radicales porque los profesionales insisten en que hay muchas redes pero sin la seguridad que ellos buscan. Entonces llegamos a un acuerdo con la OMC, en el caso del mundo médico para que nos

acreditasen que eran colegiados. Ahora mismo tenemos 12.180 registrados.
El 53% de nuestros usuarios de Ippok son médicos, el 33% farmacéuticos, el 12% enfermeros y el resto otros profesionales sanitarios. Los grandes escenarios de Ippok son, un apartado de grupos de trabajo, donde un usuario puede crear un grupo de trabajo con dos características, cerrado o abierto. Cuando te registras, al pedir la especialidad, todo se relaciona a ella. Otros grupos de trabajo son debates, eventos, la biblioteca y otro apartado de casos clínicos. A demanda se ha creado una sección de empleo. La participación es bastante estable y la tenemos en el 75% todos los meses.

La moderadora dio las gracias a los 4 ponentes por esta primera intervención. Dejó abierto el debate tanto para los ponentes como para los asistentes, pero ella, en primer lugar planteó cómo, en cada uno de los temas tratados, se contemplaba la normativa de protección de datos y cómo en cada una de las redes se daba la información, a través de una política de privacidad, mediante un cuestionario que tiene que cumplimentar y que sirva además para recabar el consentimiento. "No sé como lo hacéis cada uno". Con respecto a este planteamiento Rosario Serrano matizó que "en todo momento, incluso cuando apareció Diario Médico hace ya 20 años, nosotros tenemos que justificar ante la Comunidad de Madrid, que es donde la empresa está registrada, que somos un medio de comunicación que nos dirigimos exclusivamente a personal sanitario. Principalmente para garantizar eso y también por el aspecto publicitario ya que cuando se habla de prescripción médica, como sabéis, por la Ley General de Policía de Medicamentos no puede llegar sin comentar. Como ya partimos con ese hándicap, cualquier publicación o cualquier proyecto nuevo antes de desarrollarlo nos encargamos de pasar por la asesoría jurídica para que vayan solicitando los trámites de soporte válido que acrediten y garanticen que la Comunidad de Madrid nos va a dar permiso.

Pedro Martín comentó que él no había buscado esos remedios porque en su caso lo interpretó como una necesidad que le pedían los pacientes. Pensó que la posibilidad para ponerse al día podría ser redactar un documento diciendo que se iban a utilizar esas redes con los riesgos que conlleva. A continuación se proyectó un vídeo en el cual un paciente de Pedro Martín elogia el trato que reciben los pacientes de su médico y de su actividad y el buen uso que hacen con una app, cuyo uso facilita mucho la vida de los pacientes.

Roberto Nuño, volviendo al tema de seguridad comentó que "Kronikoen Sarea, aunque actualmente está albergado en un proveedor externo, desde el lanzamiento, toda la política de seguridad que se aplicó es homologable a la que utiliza la sociedad pública de informática del Gobierno Vasco. En el momento del registro el usuario conoce la normativa que ampara la información que va a proporcionar y además se le da la posibilidad de definir un perfil de privacidad que puede ser abierto como en el caso de Facebook o puede ser cerrado para que únicamente esté en contacto con un grupo reducido de personas. En la encuesta que mencioné antes, la percepción de confianza del personal que participa en la red es muy alta y solo un 3% de los usuarios que contestaron a la encuesta manifestaron que tenían algún tipo de incertidumbre sobre la seguridad de su información".

Antonio Delgado comentó que "en Forumclinic tienen una política que el usuario tiene que aceptar, pero también han observado que al poder funcionar con un nick y una dirección que seguramente tampoco es personal, hay veces que cuando uno mira los registros nos damos cuenta que hay datos que no casan. Es un problema que intentamos solucionar porque habrá pacientes que no quieran dejar constancia. Incluso, no se recoge ningún dato médico y ni siquiera se les pide que digan en qué foro van a participar. Hemos probado que desde Latinoamérica se mandan mensajes recomendando determinados fármacos que inmediatamente se eliminan. También quiero señalar que los usuarios no pueden compartir datos. Pueden mencionar sus estados anímicos, inquietudes y dudas pero nadie puede poner, por ejemplo, sus análisis. En nuestro caso se han aplicado todas las medidas de seguridad porque detrás estaba el hospital y para nosotros no suponía apenas coste, pero sí que es verdad que hay una barrera tremenda para que este tipo de iniciativas que son muy útiles, puedan instalarse".

La moderadora preguntó si se recibían o no quejas por parte de los usuarios.
"En nuestro caso –dijo **Antonio Delgado**– tenemos algún problema que otro, derivados de la naturaleza del foro. En el de esquizofrenia o trastorno bipolar hay momentos en que se reciben quejas, alguna de ella relacionadas con los datos, o que alguien comente el caso de otra persona. Ahí tenemos que tener en cuenta la autonomía de los que intervienen. Nosotros podemos poner unos controles para evitar que eso suceda pero es complicado, sobre

todo cuando hay enfermedades que en un momento álgido de la enfermedad en el que la persona que está escribiendo no puede comportarse de manera normal. A veces se les expulsa del foro pero es fácil volverse a dar de alta".

Pedro Martín dijo que lo que había permitido es aliviar la burocracia de la consulta y que cuando un paciente le comentaba un problema que debía ser visto en la vida real que no en la digital, veían cuál era el momento más adecuado para atenderle. "A parte de este uso que nosotros tenemos con los pacientes, hay otro grupo de médicos y profesionales que llevan a cabo otro tipo de foros y en estos sí mantenemos las medidas de seguridad y una protección de datos muchísimo mayor e incluso queremos compartir la historia clínica para buscar una solución común. Otras veces, desde mi casa nos hemos conectado por Skype y hemos conseguido solucionar el problema de una forma mas real sin tener que acudir a la consulta".

Rosario Serrano añadió que en su caso, el planteamiento es que las quejas procedían de aquellas personas interesadas en la red pero que por no dar el perfil no podían pertenecer a ella.

Roberto Nuño señaló que internamente, dentro de la plataforma, sí que había habido, además muy recientemente, una queja o una inquietud ya que, como había comentado, el dinamizador que participaba tenía una rutina de introducir dos veces por semana una serie de contenidos y de noticias y cuando hicimos la transición durante un mes no hubo esas noticias lo que generó la inquietud de que no se volvieran a publicar comentarios y noticias.

Pedro Martín comentó que en su caso tampoco se habían presentado problemas. Además tampoco le piden algo con urgencia ya que saben que él se encuentra fuera del horario laboral y no puede contestarles inmediatamente. O simplemente que estoy conduciendo. A veces atiende más pacientes que en la propia consulta. Añade a un comentario de Rosario Serrano que preguntó si tenía compañeros en contra de esta gestión y contestó que sí, sobre todo cuando se les formula alguna pregunta en su tiempo libre. Además añade, que "durante el último mes varias personas que han sido derivadas a urgencias. En su seguimiento evolutivo les expliqué en la consulta porque les había cambiado el tratamiento y posteriormente me consultaban cómo manejar los niveles en el nuevo tratamiento".

CLAUSURA



Estuvo presidida por **Francisco Javier Morrás Iturmendi,** consejero de Presidencia, Justicia e Interior del Gobierno de Navarra.

Emilio Aced agradeció al Consejero su presencia y a todos los compañeros, al Comité Organizador, al Comité Local y a todos los moderadores y ponentes que habían intervenido. "Hemos tratado aspectos de algo que ya no es el futuro. Espero que las sesiones de este foro en el que se han tratado temas tan importantes, aunque no nos hayan dado soluciones si nos han proporcionado reflexiones sobre este tema".

Luciano Sáez agradeció igualmente al Consejero su presencia. También agradeció a Juan José Rubio la inestimable ayuda prestada, a SODENA, a Juan Carlos Fernández Valdivielso, a Guillermo Vicente y a Valentín Elizondo. "Creo que la confluencia de los apoyos, tanto de las Agencias conjuntamente, con el apoyo del Gobierno de Navarra y de las empresas que nos han apoyado, han hecho posible que podamos estar aquí". Anunció Inforsalud 2014. Dijo que esperaba verles a todos por allí.

Francisco Javier Morrás agradeció la oportunidad de clausurar este acto. "Ello nos permite establecer con la SEIS una estrecha colaboración. Los que hemos participado en otro tipo de actos sabemos lo difícil que es encontrar gente comprometida para dedicar su tiempo a este acto. Agradezco que se planteen retos como los que se están planteando y que se presenten problemas, ya que es la única manera de encontrar las soluciones.

En esta materia vamos a tener que reflexionar mucho y habéis de saber que en muchas ocasiones se os va a mirar con lupa. Es muy positivo las conclusiones a las que habéis llegado ya que hay que hacer avanzar a la sociedad".

III Reunión de la Red de Responsables de Seguridad de la Información Sanitaria

PAMPLONA 19 DE FEBRERO DE 2014

RED ESPAÑOLA DE RESPONSABLES DE SEGURIDAD DE LA INFORMACIÓN DE SALUD

Juan Díaz García, Juan Miguel Signes Andreu
Coordinadores de la Red

La SEIS constituyó la Red de Responsables de Seguridad de la Información Sanitaria el 20 de marzo de 2013 en Pamplona, para que las personas que trabajan en los entornos de Salud en las distintas Comunidades Autónomas y en el Ministerio de Sanidad puedan disponer de un foro estable y permanente, patrocinado y apoyado por la Sociedad Española de Informática de la Salud, pueda compartir sus inquietudes profesionales.

En la Red podrán participar todos los profesionales del Sistema Nacional de Salud así como los pertenecientes a entidades sanitarias privadas con responsabilidades en el ámbito de la seguridad de la información. Hasta el momento, la Red de Responsables de la Seguridad de la Información de Salud, ha celebrado tres reuniones. La constitutiva, la celebrada en Oviedo y la celebrada en Pamplona durante el mes de febrero de 2014.

A la primera reunión asistieron responsables de seguridad de la información de los diferentes Servicios de Salud, miembros de la Junta Directiva de la SEIS y representantes de las Autoridades de Protección de Datos que participan como observadores.

Se establece un amplio debate de cuáles podrían ser los objetivos y líneas de actuación de la Red, señalándose los siguientes aspectos: Compartir experiencias, tener en cuenta la opinión de los responsables de seguridad de los centros, definir las funciones genérica de los responsables, elaborar informes y hacer prospectivas de cara al futuro,

Se plantea como un primer objetivo la elaboración de una encuesta de análisis de situación de la Seguridad de la Información en los entornos Sanitarios, de las diferentes Comunidades Autónomas.

II Reunión de RERSIS en Oviedo. Tuvo lugar el 10 de octubre de 2013 y asistieron los responsables de seguridad de los diferentes Servicios de Salud y miembros de la Junta Directiva de la SEIS. Durante esta Reunión se explicó por parte de Juan Díaz el espacio colaborativo web que se ha desarrollado provisionalmente, como se han implementado y la estructura básica para alcanzar unos de los primeros objetivos de la Red como es el de compartir experiencias y tener en cuenta la opinión de los responsables de seguridad

III Reunión de RERSIS en Pamplona. El 19 de Febrero de 2014, se vió incrementado el número de asistentes y se realizó la presentación de los diferentes participantes de su perfil y su centro de trabajo para facilitar el conocimiento, experiencia y expectativas. Emilio Aced Félez, informó de que el requerimiento de la Red como órgano consultivo de la SEIS es aprobado por Junta Directiva de modo que se constituye como Comité Técnico Asesor.

Posteriormente Luciano Sáez Ayerra, estableció como uno de los primeros objetivos de este Comité Técnico Asesor de Seguridad de la Información el establecer el "Modelo Organizativo de la Seguridad de la Información en los Servicios de Salud". Este documento lo remitirá la SEIS a los responsables de los servicios de salud y al ministerio. Este documento, necesariamente breve, debería enfocarse a captar la atención de esos directivos respecto a sus obligaciones en materia de seguridad de la información.

Otra línea de trabajo a desarrollar podría ser un Código Ético para los profesionales en el manejo de la información, que trasmita "confianza", evitando así las connotaciones negativas de la palabra seguridad.

Se planteó trabajar sobre el impacto de la nueva normativa europea sobre Protección de Datos desde el punto de vista de la Seguridad de la Información, y ver cómo afecta a las figuras, responsabilidades, organización, tareas, etc. Otra tarea a desarrollar tiene que ver con la concienciación de los directivos de los sistemas de salud sobre la trascendencia y el impacto de la seguridad de información en la actividad sanitaria, así como demostrar que la inversión en este ámbito es rentable mediante el cálculo del retorno de inversión que se produce.

También se planteó la necesidad de establecer un "Modelo de Mínimos" que cualquier organización debe alcanzar donde quede clara la "Separación de

Funciones" y la "Independencia" con la que debe ser desarrollada la función del control de la seguridad. Es importante trasladar los conceptos de ciberseguridad aplicados a los entornos de salud y sus implicaciones, que tienen que ser tenidas en cuenta en todos los sistemas y arquitecturas.

Se acordó realizar reuniones virtuales mediante videoconferencia con carácter mensual para facilitar el intercambio y discusión del grupo de trabajo, así como incorporar a los colaboradores de los diferentes servicios y unidades de seguridad de la información de los entornos sanitarios para potenciar su funcionamiento.

ENCUESTA SOBRE EL GOBIERNO DE LA SEGURIDAD. RESUMEN DE RESULTADOS

Juan Miguel Signes Andreu
Coordinador de la Red

Las preguntas se limitaron a 19, agrupadas alrededor de cuatro temas principales:

- Política de seguridad y normativa de desarrollo
- Reparto de tareas y responsabilidades
- Proyectos destacados en materia de seguridad
- Sugerencias y expectativas respecto a RERSIS

En cada pregunta se sugerían varias respuestas, pero se invitaba a ser creativos e incluir comentarios aclaratorios. Con esto se corría el riesgo de complicar el análisis estadístico de los resultados a cambio de una imagen más rica y representativa de la situación real.

A la encuesta respondieron 12 servicios púbicos de salud, que en conjunto atienden aproximadamente al 70% de la población cubierta por el Sistema Nacional de Salud. Los comentarios aclaratorios respondieron a lo previsto y en ocasiones trasladaron la dificultad de elegir entre una respuesta u otra.

Los resultados muestran lo siguiente:

- Existencia de una Política de seguridad de la información. Todos los Servicios Públicos de Salud que han respondido declaran disponer de una Política de seguridad de la información, si bien se constata que existen notables diferencias entre ellas.
- Publicidad de la política. En dos casos la política se ha publicado en el diario oficial de la CCAA correspondiente. En las demás es un documento interno accesible desde la intranet .
- Ámbito de aplicación. En nueve casos se trata de una norma propia del servicio de salud en cuestión. En los otros tres se aplica la política de seguridad de la información del respectivo gobierno autonómico.
- Objeto de protección. En dos casos la política afecta a toda la información que no haya sido clasificada de dominio público. En los demás, la política protege datos personales, y casi siempre con alguna otra condición: que sean datos de salud, o que estén en soporte electrónico, o ambas a la vez.
- Desarrollo de la política. Para facilitar la aplicación de la política hace falta desarrollar su contenido añadiendo mayor concreción y detalle. Todas las respuestas reconocen haber hecho esfuerzos en este sentido, pero el sentir mayoritario es que el grado de desarrollo alcanzado es insuficiente. Dos CCAA declaran haberla desarrollado extensamente.
- Marco de desarrollo de la política. Respecto a si se ha creado un marco de confianza alrededor de la política y los documentos que la desarrollan (disponibilidad de esos documentos, facilidad de acceso, compromiso de actualización, atención a las dudas, sugerencias y reclamaciones, etc), en dos respuestas se afirma haberlo hecho, mientras que en el resto se reconoce el trabajo pendiente. Normativa sobre uso del equipamiento informático de los puestos de trabajo. En la mitad de las respuestas se declara haber desarrollado esta faceta de la política de seguridad, mientras que las demás se reparten entre el desarrollo insuficiente y la ausencia de regulación. Normativa sobre el uso de servicios de almacenamiento en la nube. En esta cuestión, un tercio de las respuestas afirman la existencia de regulación, mientras que en el resto no la hay o se considera muy insuficiente.
- Normativa sobre el uso de dispositivos personales (memorias USB, tablets, smartphones...). En esta cuestión las respuestas están más igualadas, siendo la mitad las que declaran haber regulado la cuestión y la otra mitad no haberlo hecho aún.
- Reparto de tareas y responsabilidades. La mayor parte de las respuestas apuntan a que no existe un reparto de tareas y responsabilidades, y mucho menos se ha hecho público a través del diario oficial. Sólo en dos casos se afirma haberlo publicado, y al menos en uno de ellos el grado real de implantación se reconoce muy bajo.
- Personal encargado de coordinar y controlar las medidas de seguridad aplicables. En dos respuestas se declara que el número de efectivos dedicados a esas tareas, su preparación y dedicación resultan satisfactorios. En otros dos resultan ajustados pero suficientes, mientras que en resto uno o más de los tres factores está claramente por debajo de las necesidades reales.

- Plan de mejora de la seguridad. La mitad de las respuestas declaran la existencia de un plan plurianual de actuaciones en materia de seguridad de la información.
- Sistemas implantados y objetivos prioritarios. En este aspecto se observa una gran coincidencia en las actuaciones en las distintas CCAA, pero a velocidades distintas: hay lugares donde no han emprendido sistemas de autenticación basados en firma electrónica reconocida, mientras que en otros llevan años de experiencia. En otros asuntos la situación puede ser a la inversa. Las prioridades, cuando no las oportunidades, han surgido de manera independiente.
- Actuaciones propuestas para la RERSIS. Las más solicitadas se pueden resumir en dos: en primer lugar facilitar la colaboración, el intercambio de opiniones, experiencias y soluciones, y en segundo lugar emprender actuaciones destinadas a mejorar la cultura en seguridad en todos los colectivos implicados, especialmente entre los directivos.

Estos resultados permiten identificar algunos problemas comunes y obtener conclusiones:

- Las necesidades en materia de seguridad en los distintos servicios de salud son los mismos, pero hasta ahora los esfuerzos se han repetido de manera independiente (o sea, repitiendo errores y desaprovechando experiencias y soluciones ajenas). El marco normativo también es esencialmente el mismo, y las dificultades de aplicación en determinadas situaciones son problemas recurrentes. La colaboración se plantea como una buena estrategia para hacer frente a estas situaciones, en lugar de hacerlo como si en cada servicio de salud fueran los primeros, los únicos o tuvieran que hacerlo solos.
- Es necesario mejorar la cultura de la seguridad de la información a todos los niveles en cada una de las organizaciones consideradas. Esto incluye especialmente al estamento directivo y a quienes se ocupan especialmente de la seguridad, cuya dedicación y preparación dependen excesivamente de un esfuerzo personal no reconocido.
- El apoyo de la dirección es imprescindible para emprender las actuaciones necesarias en materia de seguridad, desde la implantación de un modelo organizativo basado en la separación de funciones, hasta el desarrollo de las políticas de seguridad en normas, procedimientos y guías de buenas prácticas, pasando por la verificación del cumplimiento de sus obligaciones por parte de los encargados de tratamiento.
- En cuanto al nivel de madurez en el gobierno de la seguridad de la información, los resultados indican que es todavía bastante bajo. Muchas iniciativas son el resultado de esfuerzos puntuales llevados a cabo por una o pocas personas, casi siempre vinculadas a los departamentos de informática. La alta dirección no parece haber prestado atención suficiente al gobierno de la seguridad.

Si se consideran los dos escenarios siguientes como los extremos de un continuo, la situación que describen las encuestas nos sitúa mucho más cerca del primero que del segundo:

Seguridad de la información (nivel de madurez bajo):

- Improvisación, discrecionalidad y voluntarismo.
- Cumplimiento legal como única referencia en seguridad de la información.
- Actuaciones reactivas, en respuesta a incidentes.
- La ineficiencia está asumida pero su coste rara vez se contabiliza. El recurso a la costumbre, idiosincrasia, inercia, desidia, etc es frecuente para explicar estas situaciones, e incluso para intentar justificarlas. De este modo la ineficiencia se enquista y se perpetúa.
- Actuaciones ad-hoc (incidente resuelto y a otra cosa, no se investigan las causas ni los problemas; si vuelve a suceder, se repetirá el tratamiento, o se improvisará).
- El nivel de sensibilización/participación del personal en la seguridad es relativamente bajo ("Me limito a obedecer. Ya me dirán qué quieren, y cómo").
- Desgobierno de la seguridad de la información (y probablemente, de otras actividades).

Seguridad de la información (nivel de madurez alto):

- Reparto claro de tareas y responsabilidades.
- Objetivos de control establecidos en base al cumplimiento legal y a la responsabilidad (tratamiento de riesgos).
- Actuaciones preventivas, de detección y de respuesta.
- Procedimientos de actuación definidos y aplicados.
- Actuaciones sometidas a control y mejora continua.
- El nivel de sensibilización/participación del personal en la SegInf es relativamente alto ("Sé cómo debo actuar y no necesito que me lo ordenen").

Buen gobierno de la seguridad de la información.

La transformación de nuestras organizaciones para conseguir niveles de madurez altos en el gobierno de la seguridad de la información es un trabajo arduo, donde la seguridad actúa de catalizador pero los beneficiarios son todos, desde las propias organizaciones hasta los titulares de la información y los ciudadanos en general. El papel de la RERSIS como facilitador de esos cambios está en manos de sus integrantes.

Téngase en cuenta que las respuestas a la encuesta se remitieron entre el segundo y el tercer trimestre de 2013. El Esquema Nacional de Seguridad (RD 3/2010) exige a los órganos superiores de las administraciones públicas dotarse formalmente de una política de seguridad antes del 30 de enero de 2014.


IV Reunión del Foro de Interoperabilidad en Salud
La interoperabilidad como soporte en la colaboración Socio-Sanitaria y Público-Privada
Organiza
SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD
Con la colaboración de
GENERALITAT VALENCIANA
CONSELLERIA DE SANITAT
Valencia, 7 y 8 de mayo de 2014
Centro de Investigación Príncipe Felipe
C/ Eduardo Primo Yúfera 3, 46012 Valencia
COLABORADORES TECNOLÓGICOS
AGFA HealthCare
Atos
CSC
EMC²
FUJITSU
gmv
INFORMÁTICA El Corte Inglés
intel
InterSystems
Microsoft
T-Systems

IV REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD

La interoperabilidad como soporte en la colaboración sociosanitaria y público-privada

MIÉRCOLES, 7 DE MAYO DE 2014

15:30 - 16:00 Recogida de Documentación

16:00 - 16:30 Acto Inaugural

16:30 - 17:45 PRIMERA SESIÓN
«Trabajos de normalización en el CTN139»

17:45 - 18:00 Pausa

18:00 - 19:45 SEGUNDA SESIÓN. Debate
«Colaboración Público-Privada y Socio-Sanitaria. Necesidades y oportunidades»

JUEVES, 8 DE MAYO DE 2014

9:30 - 11:00 TERCERA SESIÓN
«Actividades de investigación en interoperabilidad»

11:00 - 11:30 Pausa Café

11:30 - 13:00 CUARTA SESIÓN
«Soluciones y Aplicaciones prácticas de Interoperabilidad»

13:00 - 14:00 QUINTA SESIÓN
«Innovación TIC en Interoperabilidad en las Consejerías de Sanidad y Asuntos Sociales»

14:00 - 14:30 Clausura

SECRETARÍA TÉCNICA

CEFIC, SL C/Enrique Larreta, 5 - bajo izq. 28036 MADRID
Tel: 91 388 94 78
e-mail: eventos@cefic.es • www. seis.es


Inforfarma 2014
XI Congreso Nacional de Informática y Farmacia
CÁCERES 21 y 22 de mayo de 2014
Centro de Cirugía de Mínima Invasión Jesús Usón
Carretera N-521, km. 41,8.
10071 CÁCERES
Organiza
SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD
COLABORADORES TECNOLÓGICOS
AGFA HealthCare
Atos
CSC
EMC²
FUJITSU
gmv
INFORMÁTICA El Corte Inglés
intel
InterSystems
Microsoft
T-Systems

XI CONGRESO NACIONAL DE INFORMÁTICA Y FARMACIA 2014

MIÉRCOLES, 21 DE MAYO DE 2014

09.00 - 10.00 **Recepción de participantes** y entrega de documentación

10.00 - 11.00 **Acto Inaugural. Conferencia** ***"La modificación de hábitos y responsabilidades nuevas tecnologías en la atención sanitaria"***

11.00 - 12.30 **MESA REDONDA 1**
"Interoperabilidad de la receta electrónica del S.N.S."

12.30 - 12.45 Pausa Café

12.45 - 14.15 **MESA REDONDA 2**
"Receta electrónica para las mutualidades: S.N.S"

14.15 - 16.00 Almuerzo

16.00 - 17.30 **MESA REDONDA 3**
"Receta electrónica para mutualidades: Seguros privados"

17.45 - 19.15 **MESA REDONDA 4**
"Prescripción electrónica privada y su liderazgo por las corporaciones profesionales"

JUEVES, 22 DE MAYO DE 2014

10.00 - 11.30 **MESA REDONDA 5**
"Cumplimiento terapéutico y nuevas tecnologías: Programa Adhiérete"

11.30 - 11.45 Pausa Café

11.45 - 13.15 **MESA REDONDA 6**
"Las necesidades tecnológicas para el presente y futuro inmediato de la prescripción y de la dispensación electrónica interoperable"

13.15 - 14.15 **Acto de Clausura**

SECRETARÍA TÉCNICA

CEFIC, SL C/Enrique Larreta, 5 - bajo izq. 28036 MADRID
Tel: 91 388 94 78
e-mail: eventos@cefic.es • www. seis.es


Innovación y Salud
XXI
Jornadas Nacionales de Informática Sanitaria en Andalucía
Hacia una guía efectiva para la contratación y financiación de proyectos TIC.
Organiza
SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD
Colabora
JUNTA DE ANDALUCIA
Servicio Andaluz de Salud
CONSEJERÍA DE SALUD Y BIENESTAR SOCIAL
MÁLAGA
11,12 y 13 de junio de 2014
HOTEL SOL PRÍNCIPE
Paseo Colorado, 26
29620 Torremolinos
COLABORADORES TECNOLÓGICOS
AGFA HealthCare
Atos
CSC
EMC²
FUJITSU
gmv
INFORMÁTICA El Corte Inglés
intel
InterSystems
Microsoft
T-Systems

XXI JORNADAS NACIONALES DE INFORMÁTICA SANITARIA EN ANDALUCÍA

Hacia una guía efectiva para la contratación y financiación de proyectos TIC

Los días 11, 12 y 13 de junio se celebrarán en Málaga las XXI Jornadas de Informática Sanitaria en Andalucía bajo el lema "Hacia una guía efectiva para la contratación de proyectos TIC"

De nuevo los proveedores de salud, las empresas y los profesionales del sector TIC en sanidad intercambiarán experiencias y puntos de vista, colaborando para encontrar la mejor forma de aplicar la normativa y de movilizar los recursos disponibles para acelerar de manera efectiva la provisión y la penetración de las TIC en el sistema sanitario.

OBJETIVO

Es evidente la necesidad de facilitar el crecimiento de la penetración de las TIC en el sector salud. Ahora más que nunca, es necesario acelerar la velocidad de los cambios y ser más ambiciosos en la incorporación de las TIC en la asistencia, como factor fundamental ante los retos que se plantean en el escenario actual de cronicidad, crisis económica y personalización de los servicios.

Para facilitar dicha incorporación, los agentes que intervienen en el proceso de provisión necesitan desarrollar nuevos enfoques y nuevos métodos tanto para acelerar dichos procesos como para mejorar la eficacia de dicha provisión.

Y todo ello en el marco legal y financiero actual. Para ello se abordarán cuestiones como:

- ¿Cómo incorporar modelos de medición del retorno de la inversión en los procesos de contratación cuando las dimensiones temporales del ámbito contractual y del ámbito del impacto del proyecto no son comparables?
- ¿Cómo implementar el riesgo compartido de una manera efectiva?
- ¿Qué estrategia seguir para el fomento de modelos de compra pública innovadora y como alinearla con la estrategia completa de provisión TIC en el sistema sanitario?
- ¿Cómo acometer la contratación de renovación tecnológica necesaria actualmente en el contexto de nula disponibilidad presupuestaria para inversión y escasa en gasto corriente?

Se pretende disponer de un conjunto de recomendaciones de buena práctica para todos los agentes que intervienen en el proceso de contratación TIC, en el contexto actual de limitaciones presupuestarias y de nuevas oportunidades financieras.

Así, se plantearan los temas de colaboración público-privada, riesgo/beneficio compartido, compra pública innovadora y nuevas propuestas de soluciones alternativas o complementarias en el marco de la contratación administrativa en base a gasto corriente.

METODOLOGÍA

Retos de la contratación efectiva

Se pretende iniciar las jornadas con sesiones de enfoque docente con el ánimo de generar en la audiencia un conocimiento compartido de los asuntos en cuestión.

Posteriormente se desarrollará el trabajo de talleres paralelos sobre retos concretos, donde aplicar distintas alternativas de contratación que han requerido un trabajo previo de discusión en el tiempo de preparación de las jornadas.

Finalmente, se pretende mediante el análisis y puesta en común de las conclusiones y resultados de cada taller específico, construir un conjunto de recomendaciones como entregable tangible y disponible al final de las Jornadas.

FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS

Coordinador: **Emilio Aced**

Sexta Sesión Abierta de la Agencia Española de Protección de Datos

La AEPD presenta la Guía para una Evaluación del Impacto en la Protección de Datos Personales y abre una consulta pública sobre la misma.

La presentación se llevó a cabo en el marco de la Sexta Sesión Abierta que esta institución celebró el pasado 14 de marzo en Madrid y en ella se expusieron los puntos básicos, objetivos y características más importantes de dicha Guía además de anunciarse la apertura de un periodo de consulta pública hasta el 25 de abril. Esta consulta puede cumplimentarse a través del portal de la AEPD (www.agpd.es).

Igualmente, se respondió a las preguntas que los asistentes habían formulado por escrito en el momento de su inscripción y a las planteadas por el público tras la intervención del Director de la Agencia y de los responsables de las distintas unidades de la misma. En estas intervenciones se dio cuenta de los temas más destacados que habían sido abordados por la Agencia desde la última Sesión Abierta.

PREMIOS. Además, en el acto se hizo entrega de los premios anuales que concede la AEPD en las categorías de "Comunicación" e "Investigación", contando este último con un apartado específico para los trabajos sobre el derecho a la protección de datos en los países iberoamericanos.

Este año los premios en el apartado de "Comunicación" recayeron en las periodistas Beatriz Navarro y Mar Jiménez, por sus trabajos publicados en La Vanguardia y Cinco Días, respectivamente otorgándose un accésit a los artículos sobre protección de datos publicados por la periodista Carmen Jané en el Periódico de Cataluña.

En la categoría de "Investigación", el premio principal ha correspondido a Vicente Guasch por su trabajo 'Las transferencias internacionales de datos en la normativa española y comunitaria'. También se ha concedido un accésit a Ana Sánchez por su trabajo 'Catálogo de buenas prácticas de seguridad informática del personal sanitario'.

Finalmente, en la modalidad de investigación sobre trabajos originales e inéditos que tratan acerca del derecho a la protección de datos en países iberoamericanos, se ha premiado a la candidatura compuesta por Dolores Dozo y Pablo Martínez, por su trabajo 'Glosario Iberoamericano de Protección de Datos'.

La Agencia Vasca de Protección de Datos celebra su décimo aniversario

Con motivo del mismo, celebró una Jornada que tuvo lugar en el Parlamento Vasco y que fue inaugurada por su Presidenta, Bakarto Tejerina.

En dicha Jornada se analizó el pasado, presente y posible futuro de la Agencia así como los desafíos a los que se enfrentará la protección de datos personales en el futuro en el País Vasco, entre los que se analizaron las regulaciones de transparencia, las nuevas formas de actividad administrativa y los desafíos tecnológico que surgen cada día.
Asimismo, en el transcurso del acto se entregaron

los Premios AVPD 2014 que fueron entregaos por Josu Erkoreka, Consejero de Administración Pública y Justicia del Gobierno Vasco.
En primer lugar, se concedió una mención honorífica a Iñaki Vicuña, primer Director de la AVPD, por su dedicación y esfuerzo a la puesta en marcha de la institución.
A continuación se entregó el "Premio AVPD a una trayectoria profesional destacada y dedicada a la defensa del derecho a la protección de datos personales" que recayó en Antonio Troncoso, Director durante ocho años de la Agencia de Protección de Datos de la Comunidad de Madrid y por sus numerosas publicaciones en esta materia y, en particular, por el tratado "La Protección de Datos Personales. En busca del equilibrio", que recibió en 2010 el Premio de la Agencia Española de Protección de Datos al mejor trabajo científico.



También resultaron premiados la Asociación de Municipios Vascos (EUDEL) por promover en su actividad la garantía de la protección de datos más allá de sus obligaciones legales y el Grupo EITB por haber llevado a cabo el mejor trabajo de difusión en materia de protección de datos.

El Sistema Nacional de Salud inglés (NHS) admite que existen riesgos para la privacidad en los datos que hará públicos sobre sus pacientes

El NHS anunció a primeros de 2014 la creación de una gigantesca base de datos con los datos de sus pacientes pseudonimizados para ser utilizada por investigadores y compañías farmacéuticas. Aquellos pacientes que no quisieran que sus datos se incluyeran en la misma tendrían que manifestarlo explícitamente.

El acceso a esta base de datos tendría un coste que debería ser pagado por aquellos con Derecho a consultarla. Desde el punto de vista de los investigadores, la creación de este repositorio es bienvenida como una herramienta de gran importancia para el progreso de la investigación científica.
Ahora, el NHS ha decidido posponer la accesibilidad de la misma ante los riesgos de que, a pesar de las afirmaciones realizadas, los datos de los pacientes puedan ser re-identificados. En particular, esto podría suceder si los datos se combinaran con otras informaciones que pudieran estar disponibles aunque el NHS ha afirmado que este ataque (conocido como jigsaw attack y que podría ser llevado a cabo por hackers interesados en acceder a estos datos por múltiples razones) sería ilegal y potencialmente sancionable por la autoridad de protección de datos británica, el Information Commissioner's Office (ICO).

Otro aspecto que debe ser tenido en cuenta es que si los pacientes pierden la confianza en el Mantenimiento de la confidencialidad de sus datos de salud ello podría llevar a un empeoramiento de los servicios sanitarios dado que se podría dar el caso de que no comunicaran ciertas informaciones a sus médicos

Por otra parte, también ha habido críticas por el escaso tiempo dado a los pacientes para manifestar su oposición a ser incluidos en el nuevo sistema y por la imposibilidad de llevarla a cabo electrónicamente.

FORO DE INTEROPERABILIDAD

Coordinador: **Adolfo Muñoz Carrero**

Elaboración de una norma ISO para definir métricas de la calidad de los DCM (Detailed Clinical Models)

En el seno del TC 215 de ISO se está iniciando la elaboración de la especificación técnica ISO TS 18864 Quality Metrics for Detailed Clinical Models (Métricas de la calidad para Modelos Clínicos Detallados).

Un DCM (cuyas características, principios y procesos están establecidos en otra norma, la ISO/DTS 13972) es un modelo de un concepto del dominio clínico. En la actualidad existen varios formalismos para definir dichos conceptos, como los arquetipos de OpenEHR y la norma UNE-EN ISO 13606 o los templates de HL7 v3, entre otros. Esta variedad está causando problemas a los usuarios que no saben cuál de ellos utilizar. Los DCMs pretenden solucionar este problema subiendo un peldaño en la abstracción y ser un mecanismo para generalizar dichos formalismos en una definición común que pueda expresarse o traducirse posteriormente a cualquiera de ellos. Recientemente, la iniciativa CIMI (Clinical Information Modeling Initiative – Iniciativa para el modelado de la información clínica), inició trabajos para proporcionar dicho formato común. El objetivo es poder intercambiar las definiciones formales de los conceptos independientemente de la tecnología utilizada para su definición. De esta manera se mejoraría la interoperabilidad semántica (los sistemas podrían usar los mismos conceptos aunque fuesen heterogéneos) y las definiciones de los conceptos podrían compartirse entre distintas organizaciones y grupos de usuarios que, además, podrán contribuir a su definición y evolución mejorando su calidad.

La estrategia de doble modelo, en la que se basan los DCMs, parece ser una gran herramienta para acometer el reto de la interoperabilidad semántica, pero, evidentemente, si las historias clínicas electrónicas, los sistemas de ayuda a la decisión, los estudios estadísticos, etc. van a apoyarse en los DCMs para su correcto funcionamiento, estos tendrán que ser de buena calidad, confiables y, en el futuro, probablemente ser certificados por un organismos competente. Precisamente, la especificación técnica ISO 18864 pretende establecer unas métricas reproducibles para todos los formalismos involucrados que permitan evaluar de manera objetiva la calidad de los DCM y, por lo tanto, la de los modelos de los conceptos utilizados.

El conjunto de métricas propuestas se basa tanto en los principios que tienen los sistemas de información a la hora de incluir los modelos de los conceptos como en los principios generales de modelado. Entre ellos:

- Tiene que ser posible añadir nuevos elementos o atributos a los modelos sin tener que cambiar los programas que los tratan o los esquemas de las bases de datos donde se almacenen
- Tienen que usar un formalismo existente para su definición
- Tienen que enlazarse con terminologías normalizadas
- Tienen que tener un mecanismo para poder aseverar la negación.
- Los modelos han de representarse en lenguajes normalizados de modelado
- Los modelos deben ser compartidos y aprobados por una comunidad de expertos
- Permitir diferentes estilos de modelado que se refieran a los mismos datos clínicos y conceptos.

Siguiendo estos principios, se definen métricas en tres aspectos:

- Referentes a la estructura del DCM, que tratan del formalismo utilizado, el enlace a terminologías, el soporte para enlaces semánticos a otros DCM, los tipos de datos y la descripción normalizada de las unidades de medida.
- Referentes a la creación del contenido, que versan sobre la granularidad, reusabilidad, corrección y la amplitud de los modelos.
- Referentes al proceso de desarrollo, que controlan lo relativo a la evidencia que sostiene el modelo desarrollado, los casos de uso, los metadatos para hacer el seguimiento de los cambios y la conformidad con el lenguaje de modelado empleado

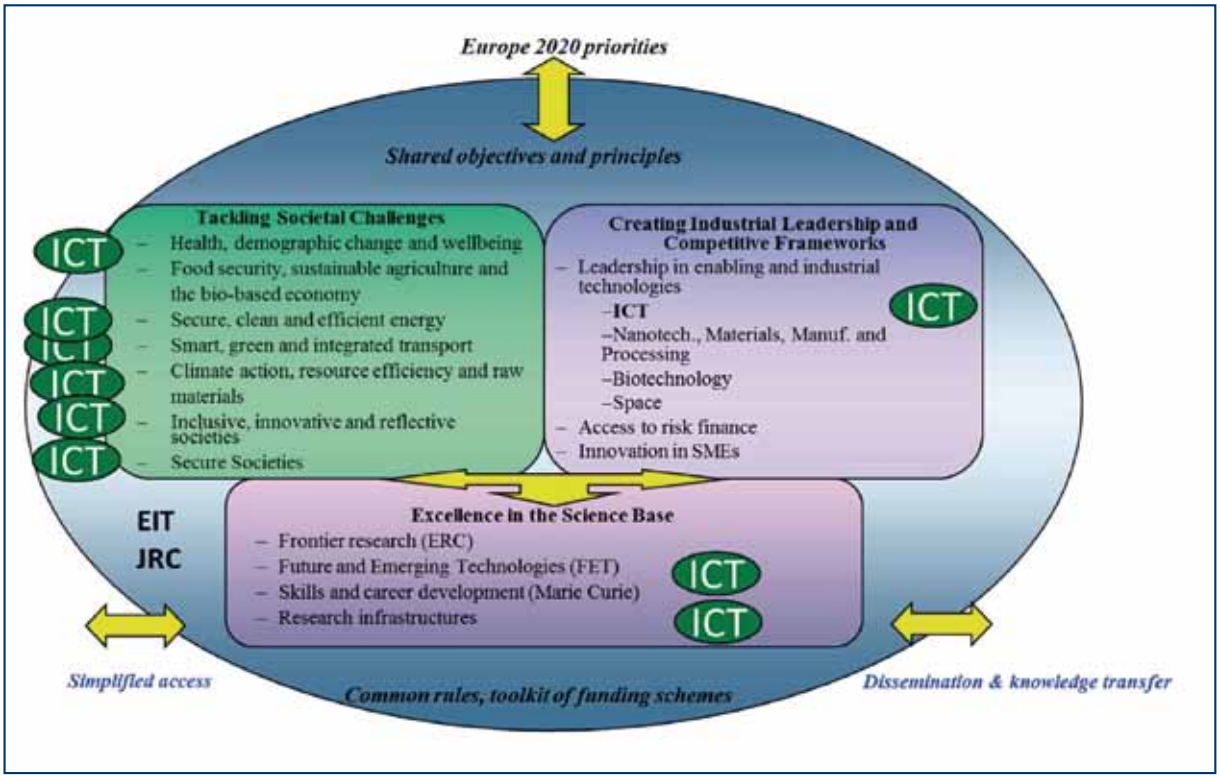
La especificación técnica se encuentra en el estado de nuevo ítem de trabajo (NWIP) y el 18 de marzo de 2014 habrá terminado el periodo de votación para ser aceptada como borrador de trabajo. España, a través del CTN139 se ha comprometido a trabajar activamente en este desarrollo.

FORO DE TELEMEDICINA

Coordinador: **O. Moreno**

Guía de actividades relacionadas con las TIC en los Paquetes de Trabajo 2014-2015 del H2020

Como tecnología genérica, las TIC están presentes en muchas de las áreas del Horizonte 2020. Se va describir una pequeña guía diseñada para ayudar a encontrar las áreas relacionadas con las TIC en las diferentes partes del H2020 y, dentro de ellas, las implicadas en temas de Salud.

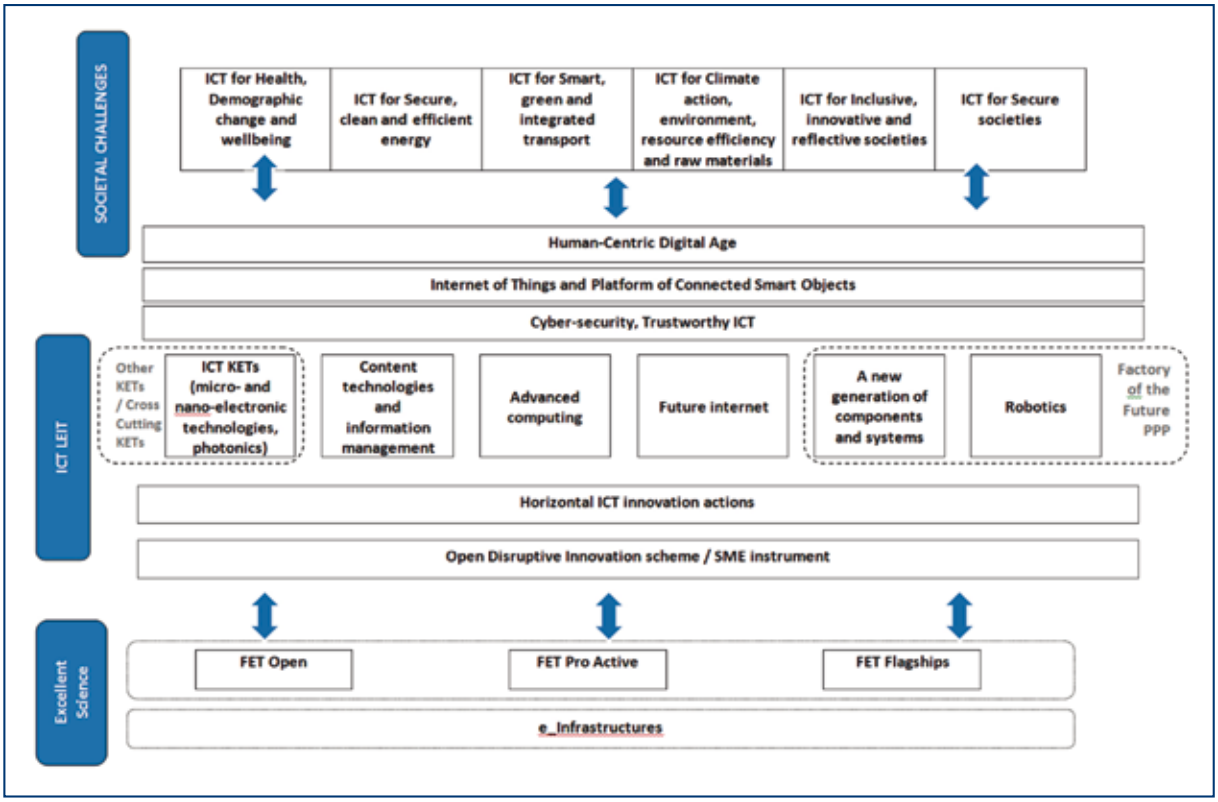


En el programa de trabajo 2014-15, los temas relacionados con las TIC están cubiertos de la siguiente manera:

- La investigación avanzada para descubrir nuevas posibilidades tecnológicas y las contribuciones de las TIC a la investigación y la innovación se abordan en la parte 'Excellent science' del programa de trabajo, concretamente bajo 'Future and Emergency Technologies', 'European research infraestructures';
- Las actividades de investigación e innovación en tecnologías, ya sea impulsados por planes de trabajo industriales o, a través de un enfoque de abajo hacia arriba se abordan en la parte del programa de trabajo de 'Leadership in enabling and industrial tecnologies' (LEIT), bajo 'Information and communication technologies';
- Impulsado por las aplicaciones de investigación multidisciplinaria y la innovación haciendo uso de las TIC, para hacer frente a los cambios sociales se abordan en los diferentes 'Societal challenges'.

Las figuras muestran una panorámica sintética de la presencia de las TIC en Horizonte 2020.

En lo que respeta a las TIC para la Salud se tratarán en el SC1: Salud, cambio demográfico y bienestar. En este punto las TIC, que tienen un papel des-



tacado en este reto social, se abordan en temas específicos en la llamada al reto "Personalización de la salud y la asistencia" (Personalising health and care –PHC-) y la llamada a las actividades de coordinación (HCO). El presupuesto total para el año 2014 es de 185,2M€ y para el 2015 de 162M€.

Las TIC contribuyen en las tres áreas siguientes de la llamada principal del SC1:

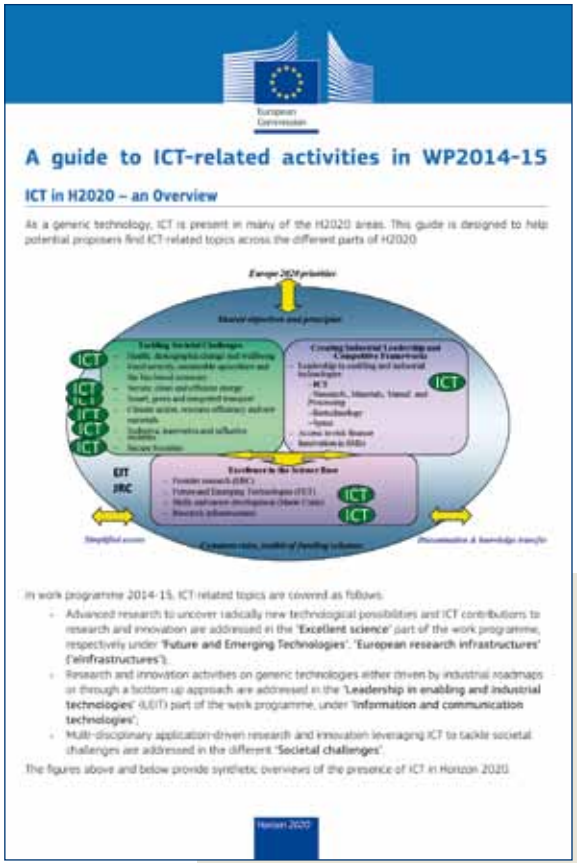
- **Envejecimiento activo y saludable.** En una población europea que envejece, los ciudadanos están en mayor riesgo de deterioro cognitivo, fragilidad y exclusión social con importantes consecuencias negativas para la independencia, la calidad de vida, la de aquellos que se preocupan por ellos y para la sostenibilidad de los sistemas asistenciales y sanitarios. Dentro de este punto las 3 líneas TIC que se llevarán a cabo serán:
  - PHC 19 – 2014: Envejecimiento activo y saludable con las TIC: robótica de servicios dentro de los entornos de vida asistidos. Alguno de los objetivos que persigue son: mejorar la calidad de vida de las personas mayores y de sus cuidadores; la evidencia de los beneficios del desarrollo de la robótica de servicios, basadas en pruebas y la participación de las partes interesadas; la reducción de los ingresos y las estancias hospitalarias y asistenciales y la prolongación del tiempo de residencia en su propio domicilio cuando el envejecimiento conlleva la aparición de impedimentos funcionales. Estiman que el presupuesto adecuado solicitado a la UE para llevar a cabo una propuesta presentada a esta convocatoria podría rondar los 3-4 M€.
  - PHC 20 – 2014: Envejecimiento activo y saludable con las TIC: soluciones TIC para una vida independiente con deterioro cognitivo. Se esperan los siguientes impactos: una clara evidencia del retorno de la inversión, tanto para el sector privado como en términos de beneficios para la sociedad con soluciones TIC para personas mayores con deterioro cognitivo; mejores prácticas para los modelos de negocio y de financiación viables y que sean escalables a toda Europa; una clara evidencia de mejoras en la eficiencia de los sistemas de salud y asistencia; una clara evidencia de mejoras en la calidad de vida y envejecimiento activo para los usuarios y cuidadores implicados; contribución a la competitividad de la industria TIC Europea, mediante la mejora de la interoperabilidad y de mercados expandibles. Se estima que con 2-3 M€ peticionados por propuesta podría ser suficiente para cumplir adecuadamente estos objetivos.

- PHC 21 – 2015: Envejecimiento activo y saludable con las TIC: detección e intervención precoz del riesgo. Presentará los siguientes objetivos: la evidencia de los beneficios de la detección e intervención temprana del riesgo, basada en prueba de concepto y la participación de las partes interesadas; mejoras claras de los resultados para las personas, los sistemas de atención y para la sociedad en general de nuevas terapias y de las intervenciones basadas en la detección temprana del riesgo en comparación con las prácticas actuales; liderazgo mundial de la innovación basada en las TIC para el envejecimiento activo y saludable. Con 3-4 M€ por propuesta podría ser adecuado.

- **Atención integral, sostenible y centrada en el ciudadano.** Apoyará el desarrollo de nuevas arquitecturas de sistemas de salud basados en modelos de atención integral que están más estrechamente orientados a las necesidades de los pacientes, a grupos de pacientes específicos (por ejemplo, estratificados y con comorbilidad) y a los ciudadanos europeos. Cinco puntos englobarán a las TIC:
  - PHC 25 – 2015: Sistemas y servicios TIC avanzados para la Atención Integral. Entre sus impactos esperados, se podrían citar: reducción de ingresos y días pasados en las instituciones de asistencia al paciente y mejoras en las actividades diarias y la calidad de vida de las personas mayores a través del uso efectivo de las TIC y de una mejor coordinación de los procesos de asistencia; fortalecimiento de la base de evidencia sobre los resultados de salud, calidad de vida y la ganancia en la eficiencia asistencial con la utilización de las TIC en la atención integrada; mejora de la cooperación y el intercambio seguro de información entre los actores involucrados en los servicios de salud, servicios sociales y los servicios de asistencia informal, etcétera.
  - PHC 26 – 2014: Autogestión de la salud y la enfermedad: la participación ciudadana y la salud móvil (mHealth).Entre otros aspectos persigue principalmente: la mejora de la autogestión de la salud, prevención de enfermedades, manejo de enfermedades y/o los gastos; fortalecimiento de la base de evidencia sobre los resultados de salud, calidad de vida, ganancia en la eficiencia asistencial y los beneficios económicos de la utilización de las TIC en los nuevos modelos asistenciales, de conformidad con los requisitos de protección de datos; aumento de la confianza en los sistemas de apoyo a las decisiones para el bienestar y la gestión de las enfermedades del paciente; fortalecimiento de la evidencia y la mejora de los conocimientos sobre el comportamiento de los individuos en relación con el bienestar, la prevención de enfermedades o facilitar la gestión de nuevas intervenciones en hábitos sanitarios personalizados. Estimaciones por propuesta de 3-5M€.
  - PHC 27 – 2015: Autogestión de la salud y la enfermedad y el empoderamiento del paciente con el apoyo de las TIC. Busca involucrar más la participación del paciente en el proceso asistencial; la mejora de la gestión de una enfermedad mediante la reducción del número de episodios y complicaciones graves; el aumento del nivel de educación y la adhesión de los individuos, los pacientes y los cuidadores relacionados con la aplicación de las TIC para la asistencia personalizada; mejora de la interacción entre los pacientes, sus familiares, los proveedores de asistencia social, sanitaria y de los cuidadores informales; reforzar el conocimiento médico con respecto a la gestión eficiente de las comorbilidades; aumento de la confianza en los sistemas de soporte a la decisión para la gestión de enfermedades/pacientes; la participación de los proveedores y autoridades sociosanitarias con un mayor compromiso en el despliegue de servicios innovadores de empoderamiento del paciente. Al igual que el anterior, una petición de 3-5M€ sería la idónea.
  - PHC 28 – 2015: Autogestión de la salud y la enfermedad y de los sistemas de ayuda a la decisión basados en modelos informáticos predictivos utilizados por el propio paciente. Persigue conseguir: mejorar la participación del paciente en el proceso asistencial; mejorar la gestión de una enfermedad mediante la reducción del número de episodios y complicaciones graves; aumentar la importancia del sector de la prevención en la asistencia sanitaria usando modelos predictivos; impulsar el desarrollo de dispositivos personales usados para la autogestión de la salud; mejorar el auto-control individual de la salud y de la prevención de enfermedades (3-5M€ por propuesta).
  - PHC 29 – 2015: La contratación pública de servicios de eSalud innovadores. Entre otros objetivos busca: la contribución al desarrollo del proceso regulatorio y legal frente a posibles barreras para la contratación de soluciones

innovadoras en la asistencia sanitaria; el uso satisfactorio y el crecimiento de la concienciación en la contratación pública por parte de los compradores para impulsar la innovación en la aplicación de las TIC en el sector de que se trate; apoyar a la interoperabilidad y a la desfragmentación del mercado; la implementación sostenible de los servicios y la creación de condiciones económicas que apoyan el desarrollo a largo plazo, etc. (1-5M€ por propuesta)

- **Mejorar la información sanitaria, la explotación de datos y proporcionar una base de pruebas para las políticas y la regulación sanitaria.** Muchas de las actividades descritas anteriormente se basan en el desarrollo de herramientas, métodos y enfoques, así como en el almacenamiento y la distribución de las fuentes de información, y por lo tanto en la integración, la normalización y la sostenibilidad de los datos. La base de pruebas para las políticas de salud pública se ve reforzada por la recogida, el almacenamiento y la explotación de los datos.
  - PHC30 – 2015: Representación digital de los datos sanitarios para mejorar el diagnóstico y tratamiento de enfermedades. Busca conseguir: un coherente y mejor uso de los datos de salud disponibles para un paciente en relación con el conocimiento médico existente en la toma de decisiones clínicas; diseño de las intervenciones predictivas y terapéuticas; una mejor gestión de las situaciones clínicas complejas; habilitar el uso de la misma información por diferentes servicios médicos y otros profesionales de la salud relevantes; mejorar el control y la coordinación entre los distintos servicios en la gestión de la salud del paciente; proporcionar una visión coherente de las necesidades de atención del paciente. Propuestas en torno a 3-5M€.
  - PHC 34 – 2014: Interoperabilidad de eSalud. Los retos que pretende conseguir son: la convergencia en el uso de las Normas de eSalud en Europa y en el mundo; Contribución al Marco de Interoperabilidad de eSalud y para el despliegue a gran escala de los Servicios de eSalud (incluyendo los transfronterizos) en Europa; en línea con la estrategia de la Unión para la cooperación internacional en la investigación y la innovación, las propuestas contribuirán a la aplicación de la hoja de ruta de la UE y EE.UU; soluciones prácticas para resolver problemas específicos y que permitan despliegues a gran escala de servicios de receta electrónica transfronterizos en la UE; contribuir a una mejor interoperabilidad semántica de los servicios de eSalud en Europa, para la construcción de un Marco Europeo de Interoperabilidad de eSalud y para preparar el despliegue de los servicios de eSalud en el marco de la iniciativa Conectando Europa; contribución para ayudar a los Estados miembros de la UE y la Red de eSalud para priorizar los casos de uso que se desplegarán a nivel nacional y para planificar mejor sus propias implementaciones nacionales. 1 M€ podría ser suficiente para las propuestas que se presenten.



MAS INFORMACIÓN

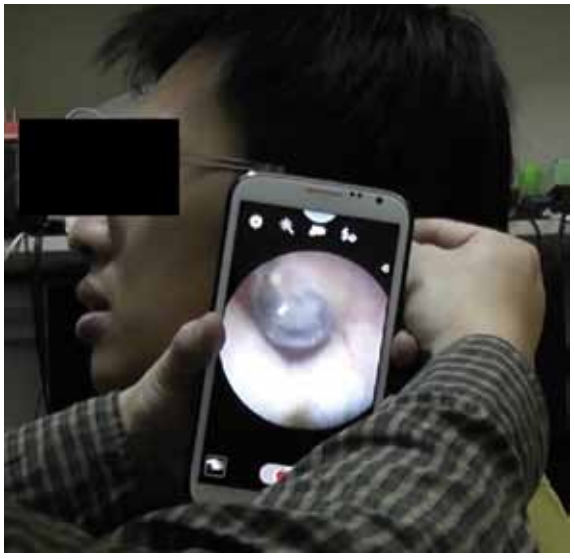
Para profundizar más en este tema consultar:
Web de la UE - http://ec.europa.eu/
Resumen disponible en: http://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/ICT%20in%20H2020%20WP2014-15_0.pdf

MEDICINA

Noticias de Informática Médica

Marcial García Rojo
Director UGC Anatomía Patológica. Hospital de Jerez, Cádiz.
Vicepresidente de la SEIS.

Jose Sacristán París
Coordinación y Sistemas Información. Área de Tecnologías de la Información. Servicio de Salud de Castilla-La Mancha.



El endoscopio conectado al smartphone para otorrinolaringología

El Hospital General de Veteranos de Kaohsiung, en Taiwán, ha diseñado un adaptador para conectar el endoscopio utilizado para oídos y nariz a un smartphone, para realizar exploraciones endoscópicas. Para ello, se adaptó la cámara del smartphone para que fuese capaz de capturar las imágenes procedentes del endoscopio. Se realizó un estudio de validación utilizando este dispositivo en teleconsulta y se obtuvo un grado de concordancia con la consulta presencial de entre un 83 y un 100%.

Fuente: Journal of Medical Internet Research. 03/03/2014. http://www.jmir.org/2014/3/e71/

El futuro de la mHealth: oportunidades de desarrollo para mantener prestaciones en épocas de crisis

Según un reciente estudio elaborado por la Sociedad Española de Médicos Generales y de Familia (SEMG) e 'iDoctus', el 42 por ciento de los facultativos de Atención Primaria usa el ordenador, las tabletas y el móvil para acceder a información médica en nuestro país. Dentro de este grupo, la inmensa mayoría (un 90 por ciento) utiliza, al menos, dos de estos dispositivos en su práctica clínica diaria. Estos porcentajes no tienen nada que envidiar a los de Estados Unidos, país de referencia en el uso de este tipo de tecnologías. En el ámbito de las aplicaciones móviles de salud, el 75 por ciento de los encuestados asegura conocer las más relevantes para su especialidad, aunque un 93 por ciento preferiría disponer de una única herramienta que englobara toda esa información. El ahorro de tiempo y la mejora en la seguridad del diagnóstico y de la prescripción son los principales beneficios referidos por estos profesionales sanitarios

Fuente: El Médico Interactivo. Enero de 2014. http://www.elmedicointeractivo.com/analisis/informes/124694/el-futuro-de-la-mhealth-oportunidades-de-desarrollo-para-mantener-prestaciones-en-epocas-de-crisis

Una aplicación informática calcula la rentabilidad de cada centro en antirretrovirales

Expertos del Grupo de Estudio de SIDA (Gesida) de la Sociedad Española de Enfermedades Infecciosas y Microbiología Clínica (Seimc), han diseñado y desarrollado una aplicación informática gratuita para medir el coste-eficacia de los tratamientos antirretrovirales contra el VIH de cada centro.

Fuente: Redacción Médica. 27/01/2014. http://www.redaccionmedica.com/noticia/una-aplicacion-informatica-calcula-la-coste-eficiencia-de-cada-centro-en-antirretrovirales-8749

Estudio sobre web de hospitales en EE UU

Un trabajo recientemente publicado ha analizado las web de 2785 hospitales estadounidenses, analizando cinco criterios: accesibilidad, contenido, marketing, tecnología y facilidad de uso. Además de ofrecer una guía sobre normalización y mejoras para sitios web, el estudio concluye que los hospitales aún no consideran su presencia online como algo estratégico en la provisión de atención sanitaria. La gestión de redes sociales se hace, generalmente, con objetivos de marketing o meramente técnicos.

Fuente: Journal of Medical Internet Research. 25.02.2014. http://www.jmir.org/2014/2/e64/

FARMACIA

Coordina: Alberto Gómez Lafón
Junta Directiva de la SEIS

Juan Luis Moreno
Responsable del Centro Coordinador de Comites Eticos de Investigación Clínica

SIC-CEIC V3

Ya en alguna otra ocasión hemos publicado en I+S lo que ha supuesto para la red de Comités Éticos de Investigación Clínica (CEICs) la operatividad del sistema de información SIC-CEIC, que se mantiene tanto a nivel funcional (Subd. Gral de Calidad de Medicamentos – Centro Coordinador de CEICs) como tecnológico (Subd. Gral de Tecnologías de la Información) por el MSSSI y en el que participan más de 130 comités éticos de toda España.

La primera versión operativa desde 2004, fue financiada por la Agencia Española de Medicamentos y Productos Sanitarios y diseñada por la Consejería de Sanidad de Cataluña, a partir de ahí, fueron esas dos unidades a las que hacía referencia y pertenecientes al MSSSI, las que han venido encargándose de su mantenimiento evolutivo. La versión 2 en 2007, la versión 3 en 2011 y su evolución no cesa. Solo a modo de reseña señalaremos algunas de las últimas incorporaciones funcionales en febrero de 2014, relacionadas fundamentalmente con la mejora en la gestión del CC-CEIC y de los propios CEICs, de las que resaltamos:

- Permitirá que el acceso al aplicativo únicamente lo puedan realizar miembros de CEICs que hayan sido marcados como gestores, excluyendo a los miembros de los CEIC de carácter más científico.
- Las tareas para los CEICs serán presentadas de forma diferente. Los gestores de los comités éticos encontrarán en el menú principal los ensayos clínicos agrupados en tres apartados: Todas las solicitudes de EC en gestión, Trabajo pendiente como CEIC Referencia (CEICR) y Trabajo pendiente como CEIC Implicado (CEICI).
- Todos los listados que puedan extraerse como resultado de las diferentes búsquedas podrán estar disponibles en formato Excel y el apartado relativo al título de la solicitud, permitirá un acceso directo a la documentación y estado del ensayo.

Otros apartados que optimizan la gestión de los protocolos y que han sido incorporados son:

- El CEICR podrá editar a los CEICI en la evaluación de cada solicitud. Hasta la fecha, modificaciones calificadas de relevantes, como la ampliación de centros de investigación implicados en el ensayo, eran informadas a todos los CEICI que participaban, pero a partir de ahora, el CEICR podrá gestionar esa ampliación únicamente con el nuevo CEIC que se incorpore al estudio.
- Se podrán seleccionar protocolos anulados al notificar cambio de estado en una solicitud en estado Evaluación y sin emitir Dictamen.
- Se añade el apartado "Conclusión Final" en la edición de las aportaciones realizadas por los CEICI y en concreto en las plantillas confeccionadas a tal efecto.
- Los CEICI solo verán su Aportación y no como hasta la fecha que podían conocer las realizadas por el resto de CEICI.
- Se incorpora un nuevo filtro para los listados de trabajo pendiente como CEICI.
- Se incorpora una plataforma de firma con tres opciones: Firma digital, Firma manuscrita escaneada y Pendiente de firma (opción por defecto).
- Para los envíos generales se dispondrá de un listado de todos los miembros, en los que se incluye un icono para aquellos que son gestores.

La legislación europea que afecta a la regulación de los ensayos clínicos va a ser modificada en el medio plazo. Los requisitos hasta el momento vigentes también sufrirán modificaciones importantes y como en otras disciplinas, aunque de forma lenta, caminamos hacia una regulación europea que afectará de forma práctica a todos los estados miembros. Para afrontar los cambios que se produzcan y para mantener nuestra vigencia y competitividad, es necesario disponer de plataformas tecnológicas flexibles y eficaces. Sin duda SIC-CEIC lo es, incluso nos atrevemos a señalar que el modelo tecnológico que debería prevalecer en la Unión Europea, debería ser muy similar a este sistema de información.

Soluciones de TI Fiables para el Ámbito Sanitario: Identificación de Deficiencias y Oportunidades

Javier Sánchez-Escribano
Responsable de Administración Pública, EMC

Los responsables de asistencia sanitaria dependen cada vez más de los registros sanitarios electrónicos y operan en un complejo contexto de gobernanza, seguridad y disponibilidad. Esto ha hecho necesario disponer de soluciones de TI fiables para el establecimiento y mantenimiento de la información sanitaria identificable de forma individual así como de la información sanitaria protegida (Protected Health Information, PHI).

Las soluciones de TI fiables para el ámbito sanitario contemplan normalmente seguridad avanzada, funciones de backup y recuperación integradas, y disponibilidad continua para la arquitectura TI de base. Los departamentos de TI se enfrentan al reto de mantener la PHI con un alto grado de disponibilidad, seguridad y privacidad a medida que incrementan el uso de la tecnología para mejorar la atención al paciente.

Los fallos de seguridad (con independencia de si los datos se guardan en sistemas TI físicos o en una nube privada) pueden generar una falta de confianza en el sistema sanitario con importantes implicaciones en la normativa.

Para evaluar las implicaciones de estos fallos en la industria sanitaria, EMC Corporation encuestó a 283 responsables de TI del sector sanitario en su estudio "2013 Global IT Trust Curve Survey" . Los resultados pusieron de relieve que las organizaciones sanitarias siguen experimentando dificultades con los tiempos de inactividad imprevistos, los fallos de seguridad y la pérdida de datos. El 40 % de los encuestados señaló que, durante los últimos 12 meses, había sufrido alguna caída imprevista del sistema por diferentes causas. Como media, estas organizaciones habían sufrido 57 horas de inactividad imprevistas, incurriendo en una pérdida estimada superior a los 300.000 euros por incidente. El estudio también reveló:

- Que el 61 % de las organizaciones sanitarias encuestadas habían experimentado al menos un incidente relativo a la seguridad en forma de fallos de seguridad, pérdida de datos o tiempo de inactividad imprevisto en los últimos 12 meses.
- Casi una de cada cinco organizaciones (19 %) había experimentado un fallo de seguridad en los últimos 12 meses con una pérdida económica media de 583.473 euros.
- Más de una de cada cuatro organizaciones (28 %) había experimentado una pérdida de datos en los últimos 12 meses, con una pérdida económica media de 581.723 euros por incidente.

El hecho de no invertir en soluciones de TI fiables para el ámbito sanitario, que protejan los datos y garanticen una red con un alto grado de disponibilidad y fiabilidad, conlleva costes cuantificables reales para el sistema de salud. Además de las implicaciones financieras, una arquitectura de TI ineficaz puede ralentizar la transición que están llevando a cabo muchas organizaciones a medida que despliegan modelos de TI como servicio (ITaaS) y tratan de entregar soluciones de TI a otras organizaciones en sus redes. Los modelos ITaaS ayudan a las organizaciones a aumentar la agilidad, acelerar el despliegue de aplicaciones sanitarias clave y reducir los costes.

Las organizaciones sanitarias tienen que cumplir con normativas tanto en Estados Unidos como en Europa en materia de seguridad y privacidad. Por eso es importante que las organizaciones sanitarias se animen a incorporar una visión global de la gestión de la seguridad mediante la adopción de un enfoque integrado de la gobernanza, el ries-

go y el cumplimiento normativo. Para armonizar las actividades de seguridad adecuadas y lograr una protección máxima en toda la empresa, es recomendable instalar un marco de gestión de la seguridad en la infraestructura de TI compuesto por:

- Gobernanza empresarial: integrando la seguridad en todos los procesos y estructuras organizacionales teniendo en cuenta los requisitos normativos y las políticas internas.

- Gestión del riesgo: identificación y clasificación de los riesgos para la información y seguimiento de la mitigación del riesgo.

- Gestión de las operaciones: implementando controles y procesos de seguridad conformes con las políticas en materia de seguridad actuales para evitar que los riesgos acaben convirtiéndose en incidentes de seguridad.

- Gestión de incidentes: detección, análisis, resolución y comunicación de los incidentes de seguridad para minimizar su impacto.

Estas estrategias se pueden implementar mediante un enfoque por fases. La inversión en una arquitectura de TI segura y fiable aumenta la confianza en las TI y mejora la atención al paciente, que debe ser el objetivo primordial en este proceso.

Ricoh e InterSystems alcanzan una alianza estratégica para ofrecer soluciones vanguardistas en el ámbito sanitario

Las soluciones interoperables conectarán dispositivos, sistemas, datos y organizaciones para mejorar sus resultados

Ricoh Americas Corporation ha anunciado una alianza estratégica con InterSystems para desarrollar nuevas soluciones de información, destinadas a la asistencia sanitaria de pacientes graves, para mejorar el flujo de trabajo, la eficiencia y la atención al paciente. Ambas empresas estarán presentes en la Conferencia y Exposición Anual HIMSS 2014, que se celebró en de febrero en Orlando, Florida (Estado Unidos).

InterSystems, líder mundial en software para la atención conectada, ofrece InterSystems HealthShare®, plataforma informática sanitaria que permite la interoperabilidad estratégica y analítica para la actuación a través tanto de una red de hospitales como de una comunidad, región o país. La alianza de Ricoh e InterSystems permitirá la disponibilidad de soluciones interoperables diseñadas para gestionar mejor la información sanitaria. La solución, de la que se ofrecerá una demo en HIMSS esta semana, hará posible que los médicos, por primera vez, puedan fotografiar la lesión de un paciente de nuevo ingreso e insertar automáticamente la imagen en su historia clínica electrónica (HCE), sin tener que alejarse de la cama del paciente. Antes de tomar la fotografía, el médico podría utilizar la cámara sanitaria Ricoh para escanear un código de barras en la pulsera del paciente y añadir información para describir la lesión. Las etiquetas pueden incluir elementos definidos por el usuario, tales como "laceración" o "pierna izquierda", la información que el médico introduzca directamente e incluso grabación de voz. La imagen fotográfica y los datos serían luego conectados de forma inalámbrica a la HCE del paciente. Esta solución crearía, rápida y fácilmente, las imágenes más completas del progreso del paciente, ofreciendo mejores resultados.

"Las lagunas de información son un gran problema en el ámbito sanitario", señala Patrick Braun, Vicepresidente del área sanitaria de Ricoh Americas Corporation. "La capacidad de capturar dinámicamente objetos de contenido no estructurado en el punto de atención, indexarlos y estructurar la información de forma inteligente, para el intercambio seguro entre las organizaciones que ofrecen la atención, incide realmente en el avance de la movilidad de la información a través del ciclo de atención del paciente. Para muchas organizaciones sanitarias, la información no estructurada sigue siendo la anti-materia de interoperabilidad y automatización de los procesos de flujo de trabajo. A través de nuestra alianza estratégica con InterSystems, estamos eliminando los silos de datos dispares, racionalizando los flujos de trabajo y suministrando soluciones innovadoras que hagan que la información trabaje para nuestros clientes del sector sanitario a nivel mundial".

En el ámbito de la fotografía, InterSystems HealthShare integra a la perfección la cámara, una HCE y la tecnología de Ricoh, empleando los estándares de la industria sanitaria incluyendo, pero sin limitarse a, Health Level Seven Internacional (HL7), Xtensible Markup Language (XML) y varios Integrating Health Enterprise (IHE), perfiles de estándares para el intercambio de información sanitaria a través de diferentes dispositivos, sistemas y organizaciones. HealthShare ha recibido la certificación, de IHE USA, de interoperabilidad TI sanitaria y de seguridad.

Agenda'14

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

IV FORO DE INTEROPERABILIDAD

Sede: Valencia

Fechas: 7 y 8 de Mayo de 2014

XI CONGRESO NACIONAL DE INFORMÁTICA Y FARMACIA "INFORFARMA 2014"

Sede: Cáceres

Fechas: 21 y 22 de Mayo 2014

XXI JORNADAS DE INFORMÁTICA SANITARIA EN ANDALUCÍA: "INNOVACIÓN Y SALUD"

Sede: Málaga - Torremolinos

Fechas: 11,12 y 13 de Junio 2014

IV FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD

Sede: Logroño

Fechas: 8 y 9 de Octubre de 2014

XII REUNIÓN FORO DE TELEMEDICINA

Sede: Valladolid

Fechas: 18 y 19 de Noviembre de 2014

III REUNIÓN PLATAFORMA TECNOLÓGICA PARA LA INNOVACIÓN EN SALUD CON LAS TIC

Sede: Valladolid

Fechas 19 y 20 de Noviembre de 2014

II EDICIÓN DEL MÁSTER EN DIRECCIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA LA SALUD

Sede: Escuela Nacional de Sanidad (ENS). Instituto de Salud Carlos III

Fechas: Septiembre 2014



2ª Edición MÁSTER EN DIRECCIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA LA SALUD

El objetivo del máster es la especialización de profesionales en la gestión directiva de las TIC en Salud en el ámbito público, privado y de las empresas proveedoras de soluciones tecnológicas, revisión de casuísticas que se producen en el ámbito de las TIC de la salud, con la presentación de casos de éxito que ayuden a su resolución.

DIRIGIDO A:

* Directivos de las Administraciones autonómicas y estatales en el área de Salud
* Directivos de organizaciones privadas aseguradoras o proveedoras de servicios de salud
* Responsables de informática, comunicaciones y sistemas de información (CIOs) de Hospitales y otras organizaciones públicas y privadas proveedoras de servicios sanitarios y sociales
* Gestores de TIC en empresas de aseguramiento sanitario
* Gestores de proyectos de TIC para la salud en empresas consultoras
* Directivos y profesionales de empresas tecnológicas proveedoras de herramientas, servicios y soluciones TIC en Salud
* En general profesionales que deseen desarrollar su carrera en la Dirección TIC para la Salud

PROGRAMA

A1: Marco de Referencia y Bases de las TIC en Sanidad

A2: Gestión Directiva de las TIC en Salud

A3: Las TIC en el Sistema Sanitario

A4: Tecnologías y Soluciones TIC en Salud

Comienzo: septiembre - octubre de 2014

Fecha de Matriculación: a partir del 1 de marzo de 2014

Duración: 2 años académicos 60 ECT´s

Metodología: Presencial y Virtual. Las clases presenciales suponen 2 días al mes (preferiblemente jueves y viernes) incluyendo las visitas y asistencia a Congresos y Jornadas Técnicas. Para aquellos alumnos que puedan tener dificultades para desplazarse a sesiones presenciales, se establecerá un programa personalizado alternativo que les permita obtener la titulación.

Institución Docente: Escuela Nacional de Sanidad (ENS) Instituto de Salud Carlos III (c/ Monforte de Lemos 1, Pabellón 8) Madrid

EQUIPO DOCENTE

Estará formado por profesionales de reconocido prestigio en el sector sanitario y tecnológico, tanto del sector público como del privado y de entidades generadoras de innovación.

Para más información e inscripción consultar www.seis.es y a través de masterdstics@seis.es

Financiación con ayudas de la Fundación Tripartita

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

Instituto de Salud Carlos III

ENS Escuela Nacional de Sanidad