DOCUMENTOS SEMFYC

Informatización en la atención primaria (I)

F.A. Alonso López (coordinador), C.J. Cristos, A. Brugos Larumbe, F. García Molina, L. Sánchez Perruca, A. Guijarro Eguskizaga, A. Ruiz Téllez y M. Medina Peralta

Palabras clave: Gestión; Informatización; Sistemas información.

Elementos de soporte conceptual

La introducción de los ordenadores en todos los ámbitos de la vida laboral es una realidad irreversible que, si bien ha procurado enormes beneficios, no siempre ha estado exenta de problemas, los cuales, aunque no vislumbrados o valorados en un principio, han dado al traste con multitud de proyectos.

La complejidad del manejo de la realidad sanitaria, generadora de infinidad de datos, obliga a contar con herramientas que nos permitan seleccionar y manejar información, en vez de datos, de una forma ágil y segura (Información = Datos × Proceso). Está claro que para la obtención y manejo de información es muy útil la informática, y esta utilidad es la que justificaría el cambio del «bolígrafo por el ordenador». Parece obvio, por tanto, que no utilizar ordenadores en la atención sanitaria es cerrarse a potenciales mejoras en el manejo de la información generada por nuestros pacientes.

En este sentido podríamos decir que un sistema de información, sanitario o de cualquier otro tipo, es un instrumento que nos permite conocer la distancia y las alternativas que poseemos para conseguir una meta que debe previamente ser definida, y su necesidad viene impuesta por la ineludible exigencia, en toda empresa, de aproximarnos a la misma *(la información* es *para la acción).*

Debe, por tanto, quedar claro que *la meta* es *la condición previa,* y *el sistema de información el instrumento de medición de limitaciones, no el fin*.

Por esta razón, nuestro punto de partida ha de ser establecer PARA QUÉ necesitamos ordenar el sistema de información, o incluso PARA QUÉ NECESITAMOS EL SISTEMA DE INFORMACIÓN mismo, dado que no definir este paso puede ser una de las causas de fracaso de la estrategia o, lo que es más grave en nuestro caso, de daño para nuestros pacientes, fin último de toda prestación sanitaria.

Nuestro *sistema de información sanitaria, por tanto, debe orientarnos hacia la meta del sistema sanitario, que* es *resolver las necesidades de salud de los individuos* y *la colectividad, definidas* en *base epidemiológica,* y *moduladas por la opinión de la población, los profesionales* y *la Administración.*

Es preciso reconocer además la especial característica de la empresa sanitaria en la que la distribución de responsabilidad se invierte respecto a otras organizaciones laborales, en las cuales la capacidad de toma de decisión y responsabilidad está concentrada en las cúspides de la organización, mientras que en nuestro entorno es en el médico de base sobre quien, en la práctica, reposan las decisiones de utilización de recursos y de establecimiento de políticas diagnóstico-terapéuticas. Conocer, respetar y asumir, la opinión y necesidades de estos profesionales parece, por tanto, un eslabón muy importante a tomar en cuenta a la hora de la elección, modulación y desarrollo de los proyectos de informatización. Podríamos decir entonces que:

La informática, en *la atención sanitaria,* es *una herramienta que, voluntariamente adoptada por los profesionales, debe contribuir a resolver con equidad y eficiencia los problemas sanitarios de los individuos y la colectividad, permitiendo diseñar sistemas de información ágiles, al hacer uso de los recursos que la tecnología de la información nos proporciona.*

Estos sistemas de información sanitaria son, si cabe, aún más sensibles que cualquiera otros ya que el objeto del proceso sanitario es directamente la intervención en personas, razón por la cual puede llegar a darse el caso que datos estrictamente dependientes de una relación, en general individual, limitada por el secreto, desborden de modo masivo el ámbito intrínsecamente privado para el que supuestamente fueron aportados.

Por ello, el establecimiento de sistemas de información en los que se vean implicados los pacientes por el uso de sus datos sanitarios ha de superar un proceso, que consideramos indispensable, iniciado por un debate social que analice las ventajas reales, no argumentos espurios, e identifique las amenazas en la potencial vulneración de los derechos de confidencialidad y de otros derechos fundamentales de la persona, y que debería seguirse de la concreción legal pertinente en cada caso específico.

En función de lo expuesto, *la herramienta informática, aun antes que* en *su diseño,* en su *propio planteamiento, ha de proteger al más débil, que es el paciente, preservando* su *intimidad, garantizando la confidencialidad de* sus *datos sanitarios y ofreciéndole ventajas palpables* en *el tratamiento de* su *salud.*

La informatización de atención primaria puede facilitar el abordaje pero, de hecho, no resuelve problemas organizativos, pues éstos deben estar resueltos previamente o, en todo caso, si con su uso se ponen de manifiesto, habremos de diseñar las estrategias operativas que permitan su solución.

Por tanto, *la informatización ha de aprovecharse como excusa para realizar o potenciar los cambios de modelo de organización sanitaria y sistemas de información que eleven al máximo la productividad del mismo* (permitiendo conocer en todo momento qué es lo que hacemos en relación

(*Aten Primaria* 2000; 26: 488-507)

a lo que costamos), y no conformarse con perpetuar modelos que se han mostrado en extremo ineficaces.
La informatización, con los condicionantes descritos, queda lejos de poder verse aisladamente como un programa; antes bien ha de contemplarse integrada en un proyecto de mejora de la atención sanitaria que postule las ventajas que han de recibir los tres agentes implicados:

– La población: contribuyendo a aumentar la calidad, la accesibilidad y la equidad de los servicios.
– Los profesionales: aumentando los conocimientos científicos y la efectividad.
– La Administración: mostrando la eficiencia y rentabilidad social (relación de las necesidades sanitarias resueltas respecto a las existentes) de las acciones sanitarias emprendidas.

Problemas y riesgos ante la informatización

Como ya se ha manifestado, las evidentes ventajas que la informatización nos puede proporcionar corren el riesgo de verse eclipsadas por las serias amenazas que pueden darse al no establecer los límites del proyecto informático, que serán éticos en mayor medida que tecnológicos, y que deben tanto evitar el uso indebido de la información por cualquiera de los 3 grupos antes citados (Administración, profesionales sanitarios, desarrolladores de programas) como asegurar que dicha información estará disponible para quien la necesite en todo momento. Entre los peligros concretos podemos destacar:

– Falta de información y consentimiento de los pacientes. No hay que olvidar que, además de reflejar los problemas del paciente, el historial clínico es un registro de actividad del propio profesional con trascendencia legal. Puede, por tanto, no ser necesario recabar el consentimiento individual explícito de cada paciente para generar una historia clínica en formato informático, pero lo que parece imprescindible es poner a disposición de todos, de forma explícita, visible y continua, la información suficiente sobre los usos y destinos de la información para permitir a cada uno de nuestros pacientes de forma individual decidir lo contrario, es decir, solicitar que dicho historial no sea informatizado.
– Efectos perversos del sistema de información sobre la propia práctica clínica. La tendencia natural de todo grupo sometido a procesos de medición y evaluación es adaptarse (positiva o negativamente según sus propios intereses, conscientes o no) a los parámetros de medición que le son aplicados. En expresión corriente, esto se traduce en *dime cómo me mides y te diré cómo me comporto.* En el caso concreto de la informatización de los sistemas de información sanitaria, la introducción de medidas de validez y fiabilidad discutibles (lo que es frecuente al medir algo tan intangible como el *producto sanitario)* podría provocar en los clínicos modificaciones en sus pautas de actuación tendentes a «salir mejor retratados en la foto». Estas modificaciones, aun sin ser significativas de forma aislada, podrían afectar de forma negativa a la atención prestada a los pacientes a corto o largo plazo. Abogamos, por tanto, por la eliminación de sistemas de información fácilmente pervertibles e ininterpretables y que, con demasiada frecuencia, constituyen la base en la toma de decisiones (dotación de recursos, productividad...) de la propia Administración sanitaria. Ítem más, la introducción de cualquier indicador debería acompañarse de un análisis exhaustivo de los riesgos, beneficios, utilidad, sentido de la tendencia y expectativas ante su aplicación (p. ej., si medimos visitas, ¿qué es lo bueno?, ¿muchas?, ¿pocas?, ¿qué propondremos ante una cifra a los centros?, ¿subir?, ¿bajar?, ¿mantener?, ¿por qué?).
– Mal uso, deliberado o inconsciente, de la utilización de la información. Los pacientes nos proporcionan información con un propósito general: que dicha información solucione un problema sanitario que les preocupa o les puede llegar a preocupar. Es frecuente encontrar cómo, bien desde ámbitos profesionales o desde la Administración, estos datos pueden, cargados o no de razones (haciendo gala de un notable *despotismo ilustrado),* intentar ser utilizados para fines que no fueron los específicos para los que se recabaron. En esta situación es preciso que *la información previa a los pacientes sobre el uso que* sus *datos sanitarios van a tener sea correcta y explícita y, que si dicha utilización no estaba prevista y comunicada en el momento de la recogida de los mismos,* se *solicite a los pacientes, que fueron quienes la suministraron, autorización expresa para dicho fin que, mientras tanto, no puede considerarse lícito.*
– Manipulación de la información. Es imprescindible asegurar que la información recogida permanece inalterada, de forma que cualquier modificación posterior, borrado o acceso a la misma es identificado y atribuible a quien fue su autor. Un sistema de control de accesos y huella riguroso ha de ser exigido para garantizar la integridad y la no manipulación de los datos recogidos.
– Dependencia secundaria a los requerimientos y fallos tecnológicos. La introducción de elementos informáticos en el entorno clínico ha de estar rodeada de una serie de medidas que garanticen al máximo su funcionamiento y disponibilidad en todo momento, y que minimicen asimismo problemas derivados de otros aparatajes o instalaciones que puedan existir. No hay que olvidar que la informatización completa de un centro de salud provoca la desaparición de otro tipo de registros y que, por tanto, si un fallo tecnológico impidiese su uso, la información sobre nuestros pacientes se vería gravemente perjudicada. La existencia de líneas eléctricas independientes, alimentadores y estabilizadores de corriente, sistemas de copias de seguridad, equipos de repuesto y contratos de mantenimiento con empresas especializadas son inexcusables si se pretende un funcionamiento óptimo.
– Falta de cultura de seguridad física y lógica de la información. La seguridad, que adelantábamos en el punto anterior, tendría poco valor si el elemento humano no está suficientemente preparado para colaborar en el mantenimiento. Debe implicarse todo el personal en el mantenimiento del sistema y detección de potenciales problemas, debiendo explicitarse en todo caso la/s persona/s responsables de cada circuito (supervisores de accesos, responsables de copias de seguridad, responsables de supervisión de mantenimiento...).
– Debilidad de los circuitos de confidencialidad asegurada. Es patente, para cualquiera que conecte con el mundo informático, que esta tecnología, aunque cada vez mas segura, no es inexpugnable, en ocasiones por problemas de índole estrictamente tecnológica *(debilidad tecnológica)* y, en otros casos, por desconocimiento o negligencia ante las normas de seguridad aplicables por parte del usua-

rio *(debilidad cultural)*. Dado que estos hechos son incontrovertibles, nuestro deber es asegurar al máximo que la información relativa a nuestros pacientes no traspasa los límites para los que fue recabada y, por tanto, aquí, como en otros ámbitos de la medicina, debería ser de aplicación la máxima del *primum non nocere.* Ante esta situación, la existencia de bases de datos centralizadas de población general que agrupen datos epidemiológicos junto a datos identificativos de paciente es rechazable (a la vez que innecesaria pues otras alternativas ofrecen iguales resultados sin los enormes riesgos que esta solución puede llegar a comportar). Es además imprescindible formar intensa y continuamente al personal en la necesidad de respetar y utilizar adecuadamente las medidas de seguridad incorporadas en los sistemas (uso de los *passwords*, derechos de acceso, restricciones...).

– Anteposición de las expectativas de la Administración a aquellas de carácter ético del profesional que le acerquen a la meta del sistema. Como ya ha sido comentado, existen al menos tres tipos de actores partícipes del sistema sanitario público: los ciudadanos, los profesionales sanitarios y la Administración. De la confluencia, o divergencia, entre los intereses de cada grupo pueden derivarse consecuencias con trascendencia positiva o negativa sobre los resultados en salud de determinadas medidas. La lógica existencia de conflicto, fruto de visiones diferentes, nunca va a poder ser eliminada siendo sin embargo imprescindible que todos los actores implicados tengan la opción de manifestar públicamente sus posiciones y, lo que es más importante, influir en la decisión final. Como en muchos otros casos, esos órganos de participación e influencia en nuestro país no están claramente definidos y, en lo tocante a las relaciones entre Administración y profesionales, en demasiadas ocasiones se sigue padeciendo un paternalismo incontestable. Dada la trascendencia del tema, la introducción de sistemas informáticos en el ámbito clínico, como ya se ha apuntado previamente, debe contar con la voluntaria participación de los profesionales, respetando su ámbito práctico y *ofreciendo alternativas posibilistas* ante los diferentes conflictos que puedan surgir, cuestión aún más trascendente cuando de lo que se está tratando es de información relativa a pacientes de cuya salud estos profesionales son directamente responsables.

– Vacío legal en la incorporación de nuevas tecnologías. El imparable y veloz desarrollo tecnológico provoca generalmente una lenta respuesta por parte del legislativo. Si bien esta respuesta es ocasionalmente prudente, en la mayoría de las ocasiones sólo traduce una incapacidad de adaptación a los nuevos procedimientos. El contacto entre el legislador y los profesionales (sanitarios y expertos en nuevas tecnologías) ha de ser permanente y, del mismo, deben surgir directrices claras que faciliten la incorporación con rapidez de los nuevos adelantos a la práctica cotidiana, evitando vacíos legales que tanta confusión e indefensión generan para las partes implicadas.

Diez propuestas/ingredientes de modelo de informatización para atención primaria

El entorno informático, en constante evolución, precisa que cualquier recomendación efectuada en este nivel sea sometida a procesos frecuentes de evaluación continua, teniendo los profesionales de base, auténticos usuarios del sistema de información, participación activa en la definición, elección, mantenimiento, evolución y proceso de implantación de las soluciones tecnológicas que se incorporen en su entorno.

El modelo que se propone debería articularse en función de los siguientes criterios:

– Orientado a la resolución de las necesidades de salud existentes, que constituyen la meta del sistema, por lo que deberá indicarnos lo que nos separa de la misma. No se trata, por tanto, de trabajar exclusivamente para los pacientes registrados en programas y protocolos, ni tampoco en exclusiva para aquellos que cuentan con registros e historias clínicas (los que utilizan el sistema); los sistemas informáticos han de poder analizar el estado de salud de la población que tenemos asignada en su conjunto (nuestra base poblacional comunitaria), permitiendo monitorizar objetivos en salud y facilitando el desarrollo de hipótesis anticipativas a las necesidades no cubiertas.

– Aquellas bases de datos que relacionen información sanitaria y datos identificativos directos de pacientes deberán estar descentralizadas, con un nivel máximo de integración que, en nuestro medio, constituye el equipo de atención primaria. Cuando especiales características de los procesos (daño potencial a la comunidad, seguimiento de prestaciones) aconsejen la unión de datos identificativos de pacientes a datos sanitarios, deberá desarrollarse normativa específica para cada proceso centralizado, limitando el nivel de agregación *al mínimo* eficiente. Como ya ha quedado reflejado en la introducción conceptual, este punto plantea uno de los principales dilemas entre ética y tecnología, pues si bien es cierto que los desarrollos técnicos necesarios para crear una base de datos central, con todos los datos sanitarios de los pacientes (de millones de pacientes), están disponibles desde hace más de 10 años, y es cierto también que en estos últimos tiempos se ha progresado enormemente en sistemas de transmisión de información, encriptación y seguridad, la verdadera pregunta es: ¿es necesaria dicha base? o, dicho de otro modo, los beneficios aportados por una base centralizada de información individuo-patología superan a los riesgos de una sola filtración interesada de la misma? Ítem más, dado que la prestación sanitaria no siempre se realiza por el propio sistema público, y esta tendencia parece acentuarse con la introducción de nuevas fórmulas de gestión (conciertos, mutuas, aseguradoras, equipos autogestionarios, fundaciones, corporaciones...), ¿se impediría el acceso a dicha base centralizada a estos elementos sanitarios que están también implicados en la prestación y por tanto tendrían suficiente justificación para recabar toda la información disponible?, ¿se obligaría a éstos a utilizar y completar información en dicha base, a pesar de que esta información no sea de la incumbencia del sistema? Es notorio que existe legislación y castigo por la violación del derecho a la confidencialidad de los datos, pero en este caso ¿existe reparación posible a los afectados si el delito se produce? La analogía con otros procesos ligados a la introducción de alta tecnología (energía nuclear, modificaciones genéticas...) es evidente; la pregunta ya no es solo: ¿cómo es de segura? La pregunta es: ¿es imprescindible?

– Modelo de historia clínica centrada en el paciente, orientada por problemas y desarrollo del curso evolutivo

en función de episodios de atención (definidos como cualquier problema sanitario verbal planteado por un paciente o detectado por un profesional desde el primer contacto de aquél con el sistema sanitario hasta su resolución, si la hubiere). En realidad este punto no es más que la traducción operativa de dos funciones básicas de la atención primaria:

1. Visión integral de la atención sanitaria, donde los problemas de un paciente no son igual a la suma de cada uno de ellos individualmente contemplados.

2. Seguimiento longitudinal de los procesos que, además de aportar continuidad en la asistencia, permite optimizar los flujos del paciente a lo largo del sistema introduciendo análisis de eficiencia (reingeniería de procesos).

– *Posibilidad de integración asistencial de todos los profesionales de atención primaria.* Ya que no es exclusivamente el médico, ni tan siquiera los profesionales sanitarios, quienes interactúan en una relación del paciente con el sistema de salud para resolver sus problemas. Es fundamental por lo tanto que cada elemento implicado tenga posibilidad de actuar sobre los temas de su competencia, mediante un acceso modular restringible, que salvaguarde aquellos datos estrictamente dependientes de una relación limitada por el secreto.

– *Capacidad de abordaje de la salud colectiva, la familia, los núcleos de convivencia y la comunidad.* Tanto de manera funcional (en el día a día de la consulta) como analítica (análisis de actividades realizadas y pendientes) es preciso que los programas identifiquen de forma automatizada las relaciones (genograma, grupos de riesgo...) que establece el individuo y que condicionan o puedan condicionar su estado de salud, o el de su grupo relacional, y las necesidades en el consumo/uso de recursos.

– *Instrumentación* de *lo necesario para la integración con otros niveles, que asegure la continuidad* de *la atención sanitaria, previa definición* de *los datos susceptibles* de i*ntercambio electrónico,* y *limitación del traspaso* de *información identificativa* de *paciente hasta el nivel mínimo eficiente.* La operativización de este punto permite prescindir completamente de bases centralizadas de información a condición de:

1. Definir el organigrama entidad-relación de la prestación sanitaria estableciendo sin ambages quién es el responsable último de la atención sanitaria a un paciente –que en nuestro sistema es el médico de atención primaria– y su localización a través de una red informática.

2. Establecer los punteros informáticos que permitan reproducir el flujo del paciente a lo largo del sistema, a través de los cuales un profesional autorizado podría recuperar –hipervínculo– de forma automática (dejando huella en cada proceso) toda la información necesaria de *un paciente individual* (sin ninguna necesidad de acceso a bases de datos colectivas).

– *Utilización* de *codificaciones afines a nuestro medio que,* en *la actualidad, deberían* de *ser las propuestas por los grupos* de *trabajo* de *la WONCA, englobadas* en *la Clasificación Internacional* de *Atención Primaria.* El trabajo diario en atención primaria, definido en más de una ocasión como *el arte* de *manejar la incertidumbre,* se beneficia extraordinariamente de la existencia de clasificaciones específicas para el mismo que permitan extraer las potencialidades de nuestro entorno con la máxima sencillez, comparabilidad entre prácticas y países y aprovechamiento de la prevalencia de los problemas cotidianos. En la actualidad, la clasificación CIAP desarrollada específicamente para este medio, con posibilidad de integración completa del proceso asistencial (razón de consulta, diagnóstico del problema, proceso clínico y proceso administrativo) se configura como el estándar para atención primaria, posibilitando asimismo integración con la CIE-9 y CIE-l0. Conformarse a estas alturas con versiones reducidas de otras clasificaciones (cuestión ya superada a través de la experiencia con la antigua CIPSAP), o pretender que el médico de cabecera se convierta en un documentalista interpretando miles de códigos (un centro de salud con una cobertura de 20.000 habitantes atiende más de 300 nuevos problemas diarios), no sólo no parece conveniente sino que, además, contribuye a alimentar la errónea idea de que la atención primaria es superponible a la atención especializada ambulatoria por el mero hecho de que sus pacientes no se encuentran institucionalizados (lo que por otro lado tampoco es cierto). Es por tanto necesario comparar, pero para ello hay que utilizar no sólo idénticas unidades de medida sino idénticos productos y medios de producción.

– Los sistemas de información que se operativicen a través de elementos informáticos deben ayudar a los profesionales, y a los servicios sanitarios a identificar, y tomar, las decisiones necesarias para la mejora de la salud, no ignorando que éstas deben cumplir criterios imprescindibles que identifiquen la calidad, la efectividad y la eficiencia de las acciones que, esos mismos servicios, hayan puesto o deseen poner en marcha. Tanto la recogida como la explotación de información que no cumpla los requisitos mencionados es perversa, y el mantenimiento de sistemas de información basados en esas premisas no sólo no contribuye, sino que en muchas ocasiones impide un correcto desarrollo de la atención sanitaria y de la distribución de recursos.

– El sustrato estructural de los sistemas de información debe permitir la elaboración de indicadores comparables externamente o, lo que es lo mismo, no importa tanto el nombre o tipo de programa informático que utilicemos como la estructuración de la información que el mismo contenga, para poder diseñar indicadores equivalentes con cualquier otro y que cumplan las especificaciones del sistema de salud.

– *Las prestaciones de las herramientas informáticas serán dinámicas por definición, por lo que aquellas con un grado mayor de desarrollo serán las que definan las referencias,* evitando contemplar la realidad como una foto fija y favoreciendo la mejora continua de los sistemas incorporados a tres niveles:

a) Tecnológico: incorporación de nuevas tecnologías suficientemente probadas en cuanto estén disponibles.

b) Funcional: mejora continua de prestaciones introduciendo nuevos desarrollos de valor.

c) Operativo: adaptación al día a día de un medio, la atención primaria, con sus propios condicionantes (tiempos de consulta, domicilios, consultas rurales, problemas no sanitarios...).

Rol de la semFYC

La semFYC, ante el fenómeno informático, ha mantenido una actitud expectante, intentando favorecer iniciativas que aproximen el mismo a la atención primaria (Internet, página web, cursos, presencia en sus congre-

sos y publicaciones, participación en foros, programas de utilidad, etc.) pero, a la vez, teniendo claro que su papel no es suplantar sino incentivar:
1. Las iniciativas que se produzcan (individuos, empresas, instituciones...).
2. La ineludible apuesta institucional.
Nuestra sociedad, ante esta herramienta, pretende asumir hacia el futuro un papel de liderazgo, enfocado básicamente a los siguientes objetivos:
– No centrase en el desarrollo de sistemas informáticos integrados propios, sino propiciar el desarrollo tecnológico, funcional y operativo de programas que existan o puedan ser creados, en un marco de libertad, mejora continua y alejado de intereses bastardos.
– Evaluar los productos desde una visión global de proyecto, emitiendo informes de adecuación al entorno profesional de la atención primaria, entendiendo el potencial interés que puede tener el que la sociedad avale los proyectos existentes o que puedan surgir.
– Promover la transformación de los documentos científicos de la sociedad a formatos que permitan su acceso directo desde programas informatizados clínicos (guías de práctica clínica, protocolos, recomendaciones, PAPPS...) para uso público.
– Promover la formación continuada en habilidades informáticas y sistemas de información.
– Participar en los foros nacionales e internacionales de informática en atención primaria.
– Generar opinión pública ante la trascendencia de las ventajas o amenazas secundarias de los sistemas de información que puedan implementarse.
– Entender la necesidad de interlocución ante la Administración y los poderes públicos, sustentada por una base ética y de servicio a la población.
– Se plantea la creación de un grupo estable de informática en la propia semFYC y, en su caso, en las sociedades federadas.

ANEXO I

Confidencialidad

Dr. C.J. Cristos

Médico de Familia. Health Informatics.

E-mail: cristos.c@ocea.es

La confidencialidad en la informatización de la atención primaria no es una extensión simple de las ideas que se manejan en la relación convencional entre el paciente y el médico y los sistemas de información tradicionales. A diferencia de la pasividad de los sistemas inertes en papel, la informática ofrece posibilidades de *miniaturización, reproducción* y *transferencia* de datos nunca vistas hasta ahora y una capacidad de *rastreo, manipulación y procesado* activo de la información que permite incluso la *creación automática de información naciente original,* como sucede con las compilaciones y los cruces de datos, o los sistemas de prospección de información.
Todos éstos son *fenómenos inéditos* nuevos que afectan directamente al paciente y a los profesionales sanitarios (médicos y enfermeras sobre todo) y por eso estamos obligados como nunca a un análisis del tema de la confidencialidad en el entorno sanitario informatizado. Hay que rellenar los vacíos conceptuales, éticos y legales que nos encontramos cada día, cuando mucha de la información que nos confían los pacientes es transcrita a multitud de ficheros automatizados (ILT, ficheros de prevalencia, prescripción repetida, citas, terminales de identificación, facturación...) si no somos nosotros mismos quienes la recogemos en su totalidad dentro de la historia clínica informatizada.
La tecnología de la información, la intimidad de la persona y la confidencialidad de sus datos, que ya casi no se conciben si no es en soporte informatizado, son un tema nuevo y candente en el mundo, y la sociedad en su conjunto va dando respuestas retrasadas y muchas veces contradictorias a situaciones desconocidas que alteran profundamente nuestro modelo de convivencia. Las repercusiones a largo plazo son difíciles o imposibles de prever. Por eso carecemos de referencias universales, verificadas y definitivas que se puedan imitar, y este anexo sólo puede aportar definiciones y propuestas razonadas para que el lector disponga de un marco conceptual en el que basarse al enfrentarse con este problema.

Datos personales, datos médicos, datos anónimos

Por definición, todos los datos médicos de una persona son datos personales, perdón por la redundancia, y a ellos se dedican las siguientes páginas. Para aclarar conceptos, transcribimos el apéndice a la recomendación N.R. (97) de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre protección de *datos médicos:*
«– La expresión "datos personales" abarca cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de *tiempo y medios no razonables. En los casos en que un individuo no sea identificable los datos son denominados anónimos.*
«– La expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de *un individuo.* Se *refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos.*
«– La expresión "datos genéticos" se refiere a todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de *un individuo o al patrón hereditario* de *tales características dentro* de *un grupo* de *individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no.*
«– La línea genética es la línea constituida por las similitudes genéticas resultantes de la procreación y compartidas por dos o más individuos.»

Es importante constatar que, en un entorno informatizado, la frontera entre un dato identificado y un dato identificable no existe a efectos prácticos. De hecho, las «bases de datos» almacenan toda la información mediante claves aparentemente ininteligibles y a nadie se le ocurre afirmar que tal información sea anónima; su significado se reconstruye mediante las tablas internas correspondientes. La sustitución de datos de identificación como nombre y apellidos por una etiqueta codificada sólo transforma los datos en realmente anónimos en aquellos entornos donde no exista *ni se pueda obtener ni construir* la referencia necesaria para restaurar o inferir la identidad original. En cualquier otro entorno, el dato debe considerarse identificado personalmente.

También deben considerarse los datos como identificados cuando se pueda reconstruir o averiguar la persona de quien proceden merced a cruces informáticos o búsquedas lógicas aprovechando la información oculta o deducible de los datos mismos; por ejemplo, un nivel hormonal o un antígeno prostático específico pueden implicar inequívocamente el sexo de una persona. Los lenguajes informáticos para la gestión de datos disponen de herramientas lógicas de una potencia asombrosa, capaces de obtener automáticamente identidades u otras conclusiones a partir de premisas aparentemente banales, siempre que se disponga de la necesaria información de consulta, referencia cruzada o encadenada.
Respecto a la información computarizada, siempre existen algún lugar y procedimiento que permite transformar la información en identificada, cuando menos el entorno donde se recogió como tal. El anonimato sólo se puede garantizar en los demás entornos cuando se excluyen de la información aquellos datos que permiten la reconstrucción de la identidad:

– No existe ni se transmite con los datos la identidad de la persona.
– Si existe o se transmite con los datos una etiqueta codificada, se garantiza la impermeabilidad de cualquier fuente que pueda ofrecer en el presente o en el futuro información susceptible de ser usada para la reconstrucción de identidades.
– Si los datos van desprovistos de todo identificador, no se registran ni se transmiten datos suficientes como para permitir la deducción de la identidad a partir de los datos mismos con los recursos disponibles en el entorno anónimo, y se garantiza que el entorno anónimo no puede compilar o desarrollar los citados recursos por sí mismo o a partir de terceros.

El tema de la criptografía, firma electrónica y secreto y seguridad de los datos es muy complejo y no es el objeto de este anexo; sin embargo, deseamos constatar que cuando utilizamos el término «etiqueta codificada» nos referimos al anonimato puro que se puede conseguir mediante los procedimientos lógicos correspondientes o los identificadores aleatorios, de manera que en el entorno anónimo resulta computacional o lógicamente imposible asociar persona y etiqueta. Perdóneseme la excursión al campo técnico, pero debe quedar claro que etiquetas de tan amplia compilación como el número de seguridad social o el DNI, o que se puedan construir a partir de datos accesibles como el CIP de la tarjeta sanitaria, no pueden considerarse anónimas en ningún entorno, pudiendo sin embargo ser anónimos fuera de determinados entornos los números de asignación aleatoria como ciertos números de historia clínica, que sólo tienen significado en los contextos que tengan acceso al fichero correspondiente.

Concepto básico: propietario, depositario y usuario

Aunque intangible, la información es un *bien* al que es aplicable el concepto de *propiedad* del modelo de sociedad al que pertenecemos, en un estado de derecho y una economía social de mercado. Su disfrute se concreta en las características de disponibilidad, integridad y, especialmente, confidencialidad de la información.
Como pasa con la propiedad de cualquier objeto, respecto a la información las personas podemos estar en una de las tres categorías siguientes (son conceptos parcialmente superpuestos):

– *Propietario de la información*: es literalmente el dueño de la misma, según el concepto de propiedad privada coherente con el modelo de economía social de mercado y Estado de derecho. El propietario de la información tiene todos los derechos sobre ésta, sólo limitados por el ejercicio sus propios derechos de rango superior, como el derecho a la vida o a la protección de la salud, y los derechos superiores de la propia sociedad, caso del derecho a la seguridad colectiva o al bien común, de un modo similar a como entendemos los derechos que emanan de la propiedad del individuo sobre otros bienes especialmente valiosos y delicados, tanto los tangibles como el propio domicilio, o los intangibles como el honor, la intimidad o la propia imagen. En relación con la información, el propietario tiene el privilegio de enajenarla, en cuyo caso sus derechos pasarían a su nuevo propietario, o cederla en depósito, en cuyo caso tiene derecho a determinar los usos de esa información y fijar los límites de su difusión y el momento de finalización de tal depósito. En resumen, el propietario tiene el máximo de derechos (disponibilidad, integridad y confidencialidad) y el mínimo de obligaciones respecto a la información. En el caso de la información computarizada, la ley determina particularmente los derechos de acceso, rectificación y cancelación de los datos, que serían ejercicios concretos del citado derecho genérico a la disponibilidad del bien «información».
– *Depositario de la información*: por cesión del propietario. Los derechos del depositario son función de las responsabilidades adquiridas ante el propietario de la información y los deberes impuestos por él, teniendo el depositario autonomía para determinar los usos de la información dentro de los limites establecidos por el propietario y respondiendo ante él. Sus principales obligaciones son las de preservar la integridad, la disponibilidad y la confidencialidad de la información. En el caso de la información computarizada, es específicamente suya la responsabilidad de garantizar el ejercicio de los derechos de acceso, rectificación y cancelación de los datos por parte del propietario.
– *Usuarios de la información*: son un subconjunto de los depositarios de la información definido por el hecho de carecer de atribuciones para determinar usos de la información. Los usuarios se limitan a conocer o utilizar los datos precisos para una función definida, estando permanentemente sometido a controles y restricciones que impiden todo uso diferente. Su principal obligación es preservar la integridad y la confidencialidad, limitándose sus derechos a que se garanticen las condiciones que permitan el cumplimiento de la función que se les exige. Se diferencian de los depositarios especialmente en que carece de obligaciones y, por ende, de derechos respecto a la disponibilidad de la información en su conjunto.

Observe el lector que en los párrafos anteriores hemos utilizado el concepto «información» y no «datos» como objeto del derecho de propiedad: los datos en sí mismos pueden carecer de significado, pero siempre contienen información, aunque sea latente. Es precisamente esa información latente y la capacidad de los ordenadores de revelarla automáticamente lo que nos lleva a establecer como objeto del derecho de propiedad a la *información en sí misma,* para evitar

que el propietario quede en situación de alienación frente a la información naciente generada por el ordenador a partir de los datos mediante cruces y referencias internas y externas; en un ejemplo simplificado, el paciente es propietario del diagnóstico de «hiperuricemia» que puede generarse automáticamente por comparación del resultado del un análisis con el intervalo de normalidad de la uricemia, hepatitis crónica (contagiosa) evidenciada por la positividad de un VHC o la información de que es diabético insulinodependiente que se deduce en un entorno administrativo por la presencia repetida de recetas de insulina.
En nuestra opinión, el punto central para determinar derechos y obligaciones respecto a la información, y para llegar a conclusiones prácticas en cuanto a la confidencialidad, reside en adscribir a cada persona y entidad a una de estas tres categorías, vinculándolas a una localización física y lógica en los sistemas en función de su capacidad *real* de acceso y control de la información: por ejemplo, un «simple operador» que se encargue de realizar copias de seguridad no encriptadas o tenga acceso a su lugar de almacenamiento habrá de definirse como *depositario* de la información, y por lo tanto habrá de asumir derechos y *obligaciones* propios de tal rango, con mecanismos de determinación de responsabilidades y sanción similares a los de un administrador de la máxima jerarquía con acceso irrestricto a los entresijos del sistema.
Esto no resolverá la actual indefinición normativa, pero al menos ayudará a determinar qué normativa aplicar y contribuirá al desarrollo de definiciones y paradigmas éticos en la propia sociedad.

El propietario

En el entorno sanitario, *«propietario»* el ser humano que protagoniza, es o crea la *realidad objetiva* –física o mental– que es simbolizada, modelada o descrita por la información; en otras palabras, el propietario es aquella persona que *produce* la información *de novo* y la sitúa por vez primera en el campo de lo conocido.
En mi opinión, el propietario de la información es casi siempre el paciente. Lo es de toda información *relativa a él* que *venga de él,* especialmente aquella información que hubiera sido desconocida si no es porque él la ha comunicado (un síntoma, un elemento de la anamnesis).
Por extensión, el paciente es propietario de toda la información primaria *recogida por un profesional* sanitario y que sea relativa a él. El médico podría ser propietario de las observaciones y los resultados de exploraciones y estudios «objetivos» practicados por él (un signo clínico, un parámetro analítico) pero, aun así, es tal el grado de obligación de transferir los datos al paciente o su representante que puede seguir considerándose al paciente como propietario de aquéllos. También debemos considerar que el paciente es propietario de aquella información *facilitada por terceros* que *afecte a* su *intimidad,* aunque tal información le sea desconocida o carezca de control sobre su fuente, salvo por ley la información de fuentes públicamente accesibles. En estos dos últimos supuestos esta propiedad por parte del paciente estaría sólo limitada por otros derechos de las personas originarias de la información, como la seguridad o salvaguardia ante daños o perjuicios ilegítimos.
La mente del profesional sanitario es el contexto referencial fundamental donde los datos del paciente se transforman en información: el médico es propietario inicial de la información *concebida y generada por él* a partir de la información primaria propiedad del paciente, sobre todo aquella información en forma de diagnósticos y recomendaciones terapéuticas, pero tiene la obligación de transmitir esa información al paciente en cuanto sea definitiva, complementariamente al derecho del paciente a exigirla. Esta consideración es extensible a la información creada por sistemas automáticos de proceso de información que, cada vez más, van complementando o supliendo a las personas, residiendo en tal caso la propiedad inicial de la información y la obligación de transferirla en el responsable del sistema informático.
En general, quien recoge una información es depositario, no propietario de la misma (salvo cuando sea aplicable el concepto de «descubrimiento en tierra de nadie»). El trabajo y los recursos materiales e intelectuales invertidos en la recogida de la información o en la neogénesis de información naciente pueden dar lugar a derechos de compensación que podrán tener forma monetaria o de otro tipo, pero no derechos de propiedad sobre la información misma. La información recogida o generada tampoco podrá ser usada como rehén o mecanismo de presión sobre el paciente para la obtención de las compensaciones legítimas.
Además de esto, y a diferencia de los sistemas convencionales en papel, la ley especifica derechos de acceso, rectificación y cancelación de la información de carácter personal residente en los *sistemas automatizados,* además de otros derechos como:

– Saber la finalidad de la recogida de datos de carácter personal y los destinatarios de la información.
– Conocer el carácter obligatorio o facultativo de las respuestas.
– Saber las posibles consecuencias de suministrar datos o de la negativa a hacerlo. «El tratamiento informatizado de los datos requerirá consentimiento del afectado salvo que la ley disponga otra cosa.»

Y otras muchas consideraciones. Sin embargo, la aplicación de esta normativa al especial entorno de los datos médicos no ha sido específicamente desarrollada ni cuenta con antecedentes prácticos hasta donde nosotros hemos podido recoger hasta el momento de redactar estas líneas (septiembre de 1999), especialmente en lo que respecta a los sistemas integrales de información sanitaria e historia clínica informatizada. Además, la propia normativa, como la propia actitud de la sociedad, presenta imprecisiones y excepciones susceptibles de interpretación contradictoria, como se comentará más adelante.

Reserva de información frente al propio paciente

En relación con la información de salud existen situaciones de necesidad y conciencia que deben poner límite vigilado al derecho indiscriminado del paciente a la propiedad y al acceso por su parte a la información relativa a sí mismo. En opinión del autor de este anexo, la ley prima la conciencia profesional respecto a la conveniencia de comunicar o no determinada información al propio paciente, en circunstancias en que pueda verse afectado un bien o un derecho superior del propio paciente, como el propio derecho a la salud o a la vida (imaginémonos una ame-

naza expresa de suicidio ante la eventual confirmación de un determinado diagnóstico). En cualquier caso, se tiene que producir necesariamente la consecución de un beneficio superior para el paciente y el profesional habrá de responder de sus decisiones ante el paciente si se da el caso, la propia sociedad y sus instituciones.

Propiedad compartida: indistinta y «llaves simultáneas»

A diferencia de los sistemas de información convencionales, los sistemas automatizados permiten la implementación real de situaciones de propiedad compartida paciente-médico, bien con titularidad indistinta o conjunta mediante procedimientos de «doble llave», con la posibilidad de establecer estatutaria o contractualmente las condiciones de uso de la información. Esta solución se debe de contemplar e implementar en el análisis y desarrollo de sistemas de información sanitaria.
El ejemplo francés es esclarecedor; el paciente puede conseguir que el acceso a sus datos clínicos hospitalarios sólo pueda realizarse mediante una clave que sólo él posee[1].

El depositario

La condición de depositario se adquiere tácita o explícitamente por comunicación o cesión activa de la información por parte del propietario o por recogida a partir del mismo (cesión pasiva), con asunción del dominio y del control sobre ella. El depositario es el garante ante el propietario (y ante la sociedad) del ejercicio de sus derechos, especialmente en cuanto a la integridad, la confidencialidad y la disponibilidad de la información y, en el caso concreto de los datos computarizados, los privilegios concretos de acceso, rectificación o cancelación de los datos.
Los derechos del depositario emanan de las responsabilidades adquiridas ante el propietario y la sociedad. Estas responsabilidades determinan el derecho a establecer y exigir las condiciones necesarias para desarrollar los usos de la información dentro de los límites de la potestad que le fue delegada por el propietario, especialmente frente a los usuarios de la información y otras personas o entidades con posibilidad fáctica de acceso a ella.
Por definición, una información puede estar en manos de más de un depositario y, si se contempla dentro de los privilegios otorgados por el propietario, un depositario puede ceder toda o parte de la información a otros depositarios y éstos a su vez a otros en cadena, respondiendo cada uno de ellos directa y subsidiariamente ante el nivel superior y el primer depositario ante el propietario. Esto es especialmente aplicable en el contexto de la información computarizada, por su miniaturización y su inmensa susceptibilidad de réplica y transferencia a distancia, que hace que hayan desaparecido muchos de los límites físicos a la difusión de la información, y que los entornos de existencia y uso legítimos de la información puedan no tener correspondencia con lugares materiales. Por eso es tan importante definir quién es depositario de la información y, en el caso de «depósito en cascada», quién es el depositario principal y responsable primero ante el propietario. Hay que subrayar aquí que la ley establece la obligación de secreto para todo el personal, sanitario y no sanitario, que haya tenido acceso a una información por ejercicio de su profesión.
En un contexto sanitario, el depositario primero y principal de la información es el profesional sanitario a quien el paciente confía la información. La obligación de secreto no se extingue con el fin de la relación profesional con el paciente, incluso la establecida a través de una relación contractual laboral o estatutaria con una entidad provisora de servicios de salud; tampoco se extingue con la incapacidad o el fallecimiento del paciente, ni con la muerte o jubilación del sanitario. El profesional habrá de garantizar que la información de sus pacientes pase a quien le sustituya (con autorización tácita o expresa de los pacientes), o sea destruida permanente e irreversiblemente. En el caso concreto del personal sanitario, la confidencialidad es una cláusula del contrato tácito que queda determinado entre él y el paciente por el mero hecho de establecer la relación profesional.
El derecho a la confidencialidad es independiente de la «calidad» de lo reservado: el profesional «no es quién» para decidir «qué» se puede revelar y «qué» no, incluso hechos aparentemente nimios: el que un administrativo o un médico conteste a la pregunta de un familiar respecto si una persona ha venido o no a la consulta o si aparece en la lista de citados tiene consideración de violación del secreto.

El depositario de la información en atención primaria: ¿el profesional sanitario o la Administración?

En el *entorno público,* la ley avala el derecho del depositario a informatizar la información personal de los pacientes, pero a raíz de la polémica suscitada en España a partir de la imposición por parte de del Instituto Nacional de la Salud de un terminal electrónico de identificación de pacientes para su uso por los médicos, ha quedado en evidencia uno de los déficit de la normativa española en cuanto la determinación de quién es el depositario primero y principal de la información del paciente: el profesional sanitario o la Administración como tal. La interpretación que subyace al comportamiento de la Administración es la de que, merced a la relación jurídica estatutaria que une al médico con la Administración, este médico es un elemento más, como un agente de la misma para el cumplimiento de sus objetivos, de forma que médico y Administración son un mismo ente frente al paciente.
Esta concepción es hija del modelo de asistencia sanitaria hospitalaria, fraccionado en especialidades, con responsabilidades parciales distribuidas por definición, y donde el paciente es consciente de que toda información que facilite a un profesional va a ser compartida por un equipo extenso y va a parar a los archivos de la institución como tal. También es una interpretación apropiada al entorno de la gestión y su aparato burocrático en relación con los funcionarios que recaban datos personales de los pacientes en el ejercicio de su función.
Esta interpretación no es compatible con la relación multidimensional integral, integrada, ilimitada y continuada de la atención primaria, que presenta características propias netamente diferentes del modelo hospitalario y su sistema de historia clínica y del modelo gerencial.
Estas características invalidan aspectos esenciales de ambos sistemas de información para su aplicación a la atención primaria, especialmente en torno al tema de la confidencialidad.

En la atención primaria, la relación médico-paciente (y paciente-profesional en general) es *personal* entre el profesional y el paciente y, en principio, es *intransferible.* El médico no actúa como pieza de la maquinaria de la Administración. Él en persona y por sí mismo es el agente y responsable de los cuidados de salud de su paciente, actuando la Administración como proveedora de recursos y fiscalizadora.

A los médicos de cabecera se nos revelan secretos que no se revelan ni a los seres más queridos, secretos que alcanzan todo su significado en la mente de unos profesionales integrados en el mismo entorno donde el paciente vive, trabaja y se relaciona. En este contexto, el paciente espera *de nosotros* una relación cerrada, privada y exclusiva. Nosotros somos los depositarios de la información que el paciente nos confía a título personal e individual, delegando asimismo en nosotros la autoridad y la responsabilidad sobre esa información frente al resto del equipo de atención primaria, la institución sanitaria en su conjunto y, por supuesto, la Administración. En un símil judicial, somos los abogados defensores, de oficio si se quiere, pero no los fiscales.

Esta aseveración parece de sentido común y es compartida por la casi totalidad de compañeros y pacientes con quienes hemos comentado el caso. También es el espíritu que subyace en el conjunto del código de deontología médica y, en nuestra opinión, en la normativa europea relativa a la protección de datos médicos. La propia legislación española, coherentemente con el artículo 18 de la Constitución[2], presenta muchos pasajes que ratifican esta interpretación.

El Reino Unido nos lleva años de adelanto en la aplicación de ordenadores a la información sanitaria, y es clarificadora su posición en el sentido de que «los clínicos son los responsables últimos de la seguridad de los datos de pacientes que [los clínicos] confían para transmisión o almacenamiento electrónico»[3]. El Servicio Nacional de Salud británico creó hace algunos años una red informática (NHS-net) para permitir la transmisión de datos. Pese a la aparente solidez teórica del planteamiento, la British Medical Association desautorizó el depósito de información de pacientes en este entorno por parte de sus miembros, en tanto no estuviesen absolutamente garantizadas las condiciones de seguridad y confidencialidad. La polémica continúa en el momento de redactar este anexo, y en este sentido puede consultarse parte del Informe Caldicott que se adjunta como complemento[4].

Necesidad y obligación de compartir información del paciente

El derecho a la confidencialidad sólo está subordinado al ejercicio de otro derecho de rango superior, como el propio derecho a la salud y el bienestar del paciente (aunque esto debería ser entendido desde el punto de vista del paciente). En beneficio de otro derecho de orden superior, puede ser legítimo e incluso obligatorio revelar un secreto profesional. Un ejemplo de esto son las interconsultas profesionales, las sesiones clínicas o la puesta en común de datos en el trabajo en equipo; aun así, se debe reservar toda la información que no sea imprescindible comunicar y, en todo caso, se tiene que producir necesariamente la consecución de un beneficio superior para el paciente.

El código de deontología médica establece en su artículo 19 que: «1. *Los sistemas* de *informatización médica no comprometerán el derecho del paciente a la intimidad.* 2. *Todo banco* de *datos que ha sido extraído* de *historias clínicas estará bajo la responsabilidad* de *un médico.* 3. Un *banco* de *datos médicos no debe conectarse a una red informática no médica.*»

Obligación de desvelar a terceros información relativa al paciente

El derecho a la confidencialidad también se halla subordinado a otros derechos superiores de terceras personas y al derecho a la preservación del bien general. Es el caso de la «declaración obligatoria de enfermedades». Sin embargo, debe tenerse en cuenta que la revelación de diagnósticos como el sida, además de vulnerar el derecho a la intimidad y la confidencialidad, pone en peligro el ejercicio de otros derechos de la persona como el derecho la educación, al trabajo o a la propia imagen.

El médico podrá o habrá de revelar con el máximo tacto y circunspección un secreto directamente a los afectados por la conducta de riesgo de un paciente, cuando exista un comportamiento por su parte para con otras personas que atente contra el superior derecho de éstas a la salud y a la vida. Cuando sea posible, se habrá de dar conocimiento al propio paciente y, ante la previsible aparición de situaciones de conflicto o violencia, se dará parte de esta circunstancia al colegio de médicos y a la justicia, bajo condiciones que garanticen la preservación del secreto.

El profesional puede tener derecho a desvelar un secreto médico en un entorno restringido *«cuando el médico* se *vea injustamente perjudicado por causa del mantenimiento del secreto* de *un paciente y éste sea el autor voluntario del perjuicio»* (art. 18.1 del Código de Deontología Médica). Esta situación debe ser tenida en cuenta en relación con la integridad de la información que se comentará más adelante y ha de ser un elemento limitante del derecho de rectificación y cancelación de datos por parte del paciente.

Datos personales para la gestión, salud pública e investigación: «Circuitos de confidencialidad asegurada»

La obligación de garantizar el derecho del paciente a la confidencialidad de su información reside en el depositario primero y principal de aquélla, que es el profesional sanitario.

Sin embargo, el entorno de la atención primaria es cada vez más complejo: la gestión de recursos y la planificación sanitaria, la garantía de calidad, las actividades de medicina preventiva y salud pública o la participación en tareas de la docencia e investigación hacen necesario que el profesional ceda a terceros parte de la información confiada por el paciente. Esta cesión es imprescindible para la misma existencia del servicio sanitario y la propia atención al paciente, por lo que el profesional está obligado a ella.

Sin embargo, esta obligación no puede servir para eximirle de su responsabilidad ante el paciente en la salvaguarda de la confidencialidad, sino para otorgarle el derecho a imponer restricciones a los depositarios sucesivos y los usuarios de la información.

Por lo tanto, la información secreta podrá difundirse dentro de un entorno institucional de confidencialidad asegurada. Este entorno deberá cumplir las siguientes condiciones:

– Que las *funciones* a que se destina la información desvelada sean *necesarias* y *legítimas*.
– Que la información desvelada sea *necesaria y pertinente* para el cumplimiento de tales funciones.
– Que la información desvelada sea sólo la *imprescindible* para el cumplimiento de esas funciones.
– Que la información circule *sólo* en el *entorno preciso,* desvelándose *sólo* a los *profesionales necesarios* y que éstos estén *sometidos* a *secreto profesional*.
– Que se garantice permanentemente el *dominio* y control de la información *dentro* de la institución y la *impermeabilidad* y la preservación del secreto *fuera* de la misma.

La Administración debe crear unos *«circuitos* de *confidencialidad asegurada»* respetuosos con estos principios. El actual sistema implica a demasiados profesionales de múltiples categorías y con competencias y obligaciones demasiado difuminadas en cuanto al sigilo, en un contexto en el que no existe tradición ni cultura seria de secreto y confidencialidad de la información.
Por otro lado, hemos de considerar que las funciones de estadística, investigación, publicación científica o docencia *no* deben gozar de un rango superior a la necesidad de preservar la intimidad de los pacientes y la confidencialidad de la información. Podrán realizarse estudios sólo a condición de que no se acceda a datos médicos *identificables* o cuyo origen pueda ser reconstruido o inferido a partir de la propia información. Si el acceso es imprescindible para el estudio, la identificación se encriptará o enmascarará debidamente, y si eso invalida los datos para el estudio, se renunciará a la recogida de la información y al estudio mismo.

Umbral de quebranto de la confidencialidad

El profesional sanitario es responsable ante el paciente de la información que confía a terceros, y ha de tener conocimiento de los destinos, usos y garantía de seguridad y confidencialidad de la información en todas las circunstancias razonablemente posibles.
Siempre existe un *«umbral* de *quebranto* de *la confidencialidad»:* siempre es posible ejercer suficiente presión sobre el depositario de unos datos hasta conseguir su revelación; por ejemplo, no se puede garantizar que un funcionario sometido a tortura en caso de guerra guarde sigilo o que el sistema informático más seguro pueda ser víctima de un procedimiento de ataque insospechado, como ha sucedido.
El objetivo que debe perseguirse es que este *umbral* de *quebranto* de *la confidencialidad* nunca quede dentro del ámbito de lo razonablemente posible. En circunstancias normales, y anormales hasta donde sea previsible, el profesional ha de tener la seguridad de que él mismo y sus depositarios subsidiarios nunca se verán forzados a revelar información del paciente. La impermeabilidad de los circuitos de información podrá garantizarse en toda situación previsible y jamás se podrá perder el dominio y control de los sustratos físicos de soporte de la información. Es decir, que el *«umbral* de *quebranto* de *la confidencialidad»* estará siempre más allá de las circunstancias razonablemente previsibles en el entorno donde circulará la información confidencial del paciente.
Sin embargo, obsérvese la incertidumbre que suscitan las siguientes notas legales: la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal en su artículo 7.3. dispone que *«los datos* de *carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones* de *interés general así lo disponga una ley o el afectado consienta expresamente»,* mientras que el 6.2. dictamina que *«no será preciso el consentimiento cuando los datos se recojan [...] para el ejercicio* de *las funciones propias* de *las Administraciones Públicas* en *el ámbito* de sus *competencias».* Respecto a la historia clínica, cuya redacción es deber y derecho del médico, el Código de Deontología Médica, en su artículo 15.3, afirma que *«las historias clínicas se redactan y conservan para facilitar la asistencia del paciente.* Se *prohíbe cualquier otra finalidad, a no ser que* se *cumplan las reglas del secreto médico y* se *cuente con la autorización del médico y del paciente»,* a la vez que existen precedentes, como la sentencia del Tribunal Constitucional STC 37/1989, de 15 de febrero, en la que se afirma que el secreto profesional no se vulnera cuando el juez ordena la entrada y registro de un centro sanitario en el que supuestamente se llevan a cabo actividades delictivas *«para identificar y, en* su *caso, recoger lo que interese a la instrucción».*
Los textos legales evolucionados presentan una calculada ambigüedad, que es la que permite la necesaria elasticidad de las normas en el momento en que el juez las interpreta y las aplica al caso concreto, dentro de límites perfectamente establecidos. Sin embargo, y respecto a la información automatizada, las definiciones son tan inciertas y sus excepciones tan amplias y abiertas que la normativa será de poco valor hasta que la jurisprudencia siente las bases para su interpretación o se cree nueva normativa. En opinión del autor de este anexo, y en el momento de redactarlo, hay una notable confusión respecto a la manera de entender los derechos y deberes de la Administración y otras entidades para con la confidencialidad de la información, los destinos, usos, condiciones y límites de movimiento de la misma y lo que se entiende por condiciones razonables de seguridad.
Esta situación, en el momento de redactar este anexo y para el entorno de la Administración pública, implica que el *«umbral de quebranto de la confidencialidad»,* al menos para los datos informatizados, podría estar dentro de lo posible o incluso dentro de lo esperable, pudiendo estos secretos ser utilizados por la propia Administración, al margen o en contra del paciente o podrían ser desvelados a personas o entidades ajenas o potencialmente opuestas a los intereses del paciente, todo ello sin conocimiento de éste y, según interpretación de la propia Administración, sin que el paciente tenga derecho a ser informado y sin que sea preceptivo pedir su consentimiento.
Ante esta situación, los profesionales de atención primaria podríamos actuar del siguiente modo: cuando el *«umbral de quebranto de la confidencialidad»* se encuentre dentro de los límites de lo esperable, debemos exponer este hecho al paciente para que pueda tomar una *decisión informada* respecto a la conveniencia de facilitar información *antes* de facilitarla.
No se trata de obtener su «consentimiento informado», puesto que no se nos permite siquiera ofrecer al paciente la oportunidad de otorgar tal

consentimiento, sino que se trata de informarle de la existencia potencial o real de unas circunstancias en las que su información podría ser o será revelada, a fin de que el paciente pueda usar el último recurso para proteger su intimidad, que es no facilitar la información misma. Perdóneseme el símil, pero se trata de algo parecido a la lectura de sus derechos que se le hace a un detenido, constatando que todo lo que pudiera decir o hacer podrá ser usado en su contra. El terreno es resbaladizo, por cuanto que el paciente deberá ser informado también de la obligatoriedad o no de facilitar la información y de las consecuencias en caso de que se la reserve.

Un caso parecido es el del profesional que ya conoce un secreto cuando llega el momento de registrarlo: el profesional debe decidir por sí mismo o comentar con el paciente la conveniencia de no anotar la información confidencial en soportes no seguros, conservándola exclusivamente en la memoria con todas sus limitaciones.

Vulnerabilidad de la información: las bases de datos centralizadas

La impermeabilidad de todo sistema de información depende de la presión a la que esté sometida la información que contiene. En el caso de los datos médicos la presión aumenta con la cantidad de información y su exhaustividad, siendo mayor cuando más concentrada y miniaturizada se encuentre. El riesgo de que un sistema sea violado y la información pueda escapar crece exponencialmente con esta presión, mientras que las posibilidades de protección sólo crecen lineal y discretamente. La presión puede llegar a ser incontenible porque el valor de la información puede ser excepcionalmente elevado, sobre todo para intereses espurios (recientemente tuvimos ocasión de comprobar los problemas que un paciente tuvo para pedir un crédito para la compra de un vehículo a causa de que, en su buena fe, el paciente había rellenado un formulario de la entidad bancaria en el que le preguntaban las medicinas que tomaba, que en su caso incluían un medicamento con levomepromazina, un fármaco antipsicótico).

La información de carácter personal a la que estamos haciendo referencia es especialmente delicada, sensible y trascendente. En el contexto de la atención primaria y siendo nosotros, los profesionales, los depositarios y responsables de la misma, no puede recabarse, ni por supuesto registrarse o comunicarse, salvo que resulte imprescindible para el cumplimiento del fin para el que se recoge, en nuestro caso el cuidado de la salud y el tratamiento de la enfermedad. Este principio es válido para los sistemas de información convencionales sobre papel, pero resulta especialmente importante en los sistemas informatizados, donde la velocidad y las posibilidades de miniaturización, copia, transmisión, manipulación y proceso son incomparablemente superiores.

La presencia de información personal confidencial está plenamente justificada en los sistemas de historia clínica, informatizados o no, porque en las manos del médico y enfrente del paciente cumple directamente la función para la que se obtiene, es necesaria y es pertinente. Sin embargo el médico debe ser especialmente estricto con los sistemas de tratamiento automático de los datos en cuanto a la pertinencia o no de registrar y procesar información, sobre todo la de carácter personal, y ha de tener en especial consideración el sustrato físico y lógico donde se almacenan estos datos.

Los clínicos somos los responsables últimos de la información de nuestros pacientes que depositamos en los registros. En los sistemas convencionales de historia clínica y registro en papel los profesionales tenemos conocimiento directo de la solidez del lugar donde depositamos la información de nuestros pacientes, pero para entender los sistemas informatizados es necesario un conocimiento técnico que normalmente escapa a nuestro ámbito de formación. Esta situación no exime de responsabilidad al sanitario sino que, al contrario, le obliga especialmente. Esto es esencialmente válido cuando el sistema de información tiene la complejidad y el tamaño de un sistema centralizado de ámbito regional o estatal.

Cuando un sistema es grande y centralizado, basta que su información se filtre *una sola vez* para que los daños sean catastróficos e irreparables. Por la naturaleza de la información computarizada, en segundos o minutos se pueden hacer réplicas de un archivo informático entero o transmitirlo al otro lado del globo. Una vez perdido el control de la información, sus consecuencias serán ineluctables e irremediables, con la agravante de que la posesión espuria de la información será probablemente indetectable e imposible la restauración de la situación original.

No debemos olvidar tampoco la posibilidad de que los datos médicos de las personas puedan servir para usos aberrantes que se han visto y se siguen viendo en lugares no distantes, como los planteamientos eugenésicos o los fenómenos de genocidio y limpieza étnica.

Pese a lo que acabamos de decir, también es cierto que de los registros médicos computarizados se puede obtener información muy valiosa para el bien de los individuos y la sociedad. Del mismo modo, tampoco deberíamos renunciar a la centralización de algunos datos, cuando la relación riesgo/beneficio para el individuo y para la sociedad así lo justifiquen. También es necesario el recabamiento de la información imprescindible y pertinente por parte de la Administración para el cumplimiento de sus funciones legítimas. ¿Nos estamos contradiciendo?

Los sistemas de información descentralizados o distribuidos

Los objetivos que acabamos de declarar son compatibles con un modelo distribuido de sistema de información sanitaria e historia clínica, basado en soluciones creadas e implementadas localmente en condiciones de libre concurrencia, modulada por el papel director, normalizador y fiscalizador de las instituciones y los poderes públicos y las sociedades científicas y profesionales. En cuanto a la confidencialidad de los datos computarizados, los procedimientos de seguridad física y lógica que se pueden implementar en los medianos y pequeños sistemas de nivel local son actualmente idénticos a los que se pueden establecer en los grandes sistemas, siendo estructuralmente igual o incluso más consistentes que ellos, y los procedimientos de monitorización y control de las actividades del personal pueden ser prácticamente los mismos, todo ello mediante alternativas excepcionalmente asequibles, técnica y económicamente.

El sistema de información descentralizado basado en pequeños sistemas desagregados residentes en los con-

sultorios y los centros de salud tiene una característica estructural intrínseca que contribuye a garantizar la seguridad y la confidencialidad: la cantidad de la información que almacena cada sistema es pequeña y, desde una visión de conjunto, sólo representa una pequeña parte del objeto de posibles intereses espurios. Para un posible interesado en un acceso ilegítimo, la información se encuentra repartida en multitud de pequeños lotes de poco valor, cada uno de ellos bajo la responsabilidad de un depositario, un médico por norma, sometido a sus principios éticos y a todo el peso de la ley.

La recopilación ilegítima y sobre todo clandestina del conjunto de una información distribuida en múltiples lugares sería técnicamente muy difícil e imposible en la práctica. También exigiría corromper a miles de profesionales en vez de a uno solo. Además la tentación no podría ser fuerte porque sería exiguo lo que se podría ofrecer a cada uno a cambio de unos pocos datos, cuya revelación por otro lado significaría un castigo casi idéntico al que sufriría el responsable de una revelación masiva de datos.

Para la Administración pública esta descentralización no debe suponer ningún problema, por cuanto la información pertinente le llegará puntual al lugar oportuno, debidamente encriptada y desposeída de toda identidad no imprescindible. Para comprometer la confidencialidad en el grado mínimo posible o para no comprometerla en absoluto, existen múltiples soluciones técnicas que pueden aplicarse, como la utilización de claves (realmente) anónimas en los datos que se transmitan, por ejemplo, las obtenidas mediante algoritmos específicos de encriptación y firma electrónica, cuya identidad sólo podría revelarse en el sistema originario o en sistemas determinados por éste o, con muchos más peligros, en un repositorio central de identidades de absoluta garantía bajo el control conjunto y fiscalización de los poderes del estado democrático.

El sistema de información descentralizado supone una democratización de la información, que se encuentra así bajo un control más próximo e inmediato por parte del depositario principal de los datos y, en última instancia, mucho más cerca de su propietario, que es el paciente. La centralización y la uniformización del sistema de información sanitaria, especialmente de la historia clínica, a niveles superiores al del equipo de atención primaria, sobre todo a escalas regionales o estatales, no es compatible con el modelo de sociedad al que pertenecemos, siendo sin embargo propio de sistemas totalitarios superados por la historia.

La integridad, complemento de la confidencialidad

La integridad de la información es un aspecto de los derechos del propietario y del depositario de la información. Este anexo se refiere a la confidencialidad de la información, por lo que sólo vamos a tratar de su integridad en cuanto a un aspecto: el derecho de acceso del propietario en los casos de litigio, malpraxis y similares.

Salvo en los casos que se ha comentado, el paciente tiene derecho a acceder a la información que le pertenece, y en tal sentido le pertenecen las notas clínicas del médico en cuanto a que son conclusiones y referencias atribuidas al paciente y estén registradas en la historia clínica. Entendemos que el profesional puede reservarse sus borradores y sus conjeturas abstractas no personalizadas, pero éstas, en general, no se anotan en la historia clínica.

Al igual que en el papel, es necesario poder corregir o tachar (nunca eliminar) una información incorrecta, por ejemplo, una errata en la transcripción de datos o una nota clínica de un paciente en la historia de otro paciente. Pero desde el punto de vista del paciente, la historia clínica tiene carácter de acta documental que registra la actividad del médico con relación a él, y por ese motivo nunca se pueden eliminar anotaciones que ya están hechas.

La ley exige que todo aquello que se tache, borre o modifique en una historia clínica pueda seguir siendo legible en el futuro, y los sistemas computarizados de historia clínica deberán responder a este requerimiento, bien mediante el resalte de los datos modificados mediante una característica distintiva (por ejemplo, cambio de color o densidad del trazo) o mediante el almacenamiento oculto del original inmodificado y sus posibles modificaciones sucesivas junto con un mecanismo «bajo llave» de reconstrucción retrospectiva y presentación de la versión original, mostrándose en condiciones normales únicamente la última versión válida junto con una señal que haga evidente que se trata de una modificación.

Menores e incapacitados. Situaciones especiales

Los padres y tutores no representan a los menores en aquellos derechos que pueden ejercitar por sí mismos, entre ellos el derecho al secreto y confidencialidad de su información sanitaria. Respecto a este principio, la mayoría de edad no es una fecha precisa, sino que depende de la madurez del paciente, a juicio del sanitario, respecto al tema de que se trate, y en caso de que el menor sea considerado maduro, el profesional habrá de sujetarse a las mismas obligaciones que con una persona mayor de edad, incluso frente a sus padres o tutores. Obviamente, el sanitario habrá de responder de sus juicios profesionales respecto a la madurez de un menor, pero no del hecho de mantener la confidencialidad de la información.

Un tema delicado por falta de definición legal es el de los menores netamente inmaduros, por lo tanto «sin derecho» preciso a la confidencialidad. Creemos que se trata de una situación que puede resolverse por reducción al absurdo: si el menor teme que un dato clínico pueda ser revelado a sus padres o tutores, no comunicará la información y por lo tanto no existirá el secreto cuya confidencialidad que se quiere negar. Frente a padres y tutores, el resultado final es el mismo que cuando el médico conoce y garantiza el secreto, con la diferencia de que en este último caso el pequeño paciente puede ser ayudado, mientras que en la primera circunstancia el menor se quedaba en situación de desamparo, a solas con su secreto.

Es una paradoja: la injerencia por parte de padres y tutores destruye las condiciones necesarias para que el pequeño paciente comunique al médico la información misma sobre la cual ejercitar el derecho de revelación. Esto crea un círculo vicioso que sólo se resuelve protegiendo la confidencialidad del secreto del menor, incluso en contra del derecho de padre o tutor. La consecuencia de actuar de otro modo sería el desamparo del menor, quien incluso puede recurrir a buscar ayuda sanitaria fuera de los circuitos asistenciales formales.

No es bueno impedir que unos padres tengan conocimiento de un problema de su hijo; sin embargo, sería peor que el menor no tuviera alternativa posible y se sintiera forzado a seguir ocultando su problema y que, finalmente, nadie le pudiese ayudar con garantía razonable.
Este mismo razonamiento es generalizable. Para poder ejercitar el derecho a que se revele una información secreta, primero es necesario que exista ese secreto gracias a que el paciente lo haya confiado, pero para que el paciente confíe un secreto primero es necesario que tenga garantizada la confidencialidad del secreto. Si no se garantizase la confidencialidad, los secretos no serían confiados y los pacientes se quedarían solos y desamparados con sus secretos. Es una argumentación complementaria a lo comentado en páginas anteriores al hablar del *«umbral* de *quebranto* de *la confidencialidad».*
En la vida profesional de los médicos se producen casos de conflicto y situaciones límite entre el deber de secreto y la obligación de comunicar una información clínica, y es que a veces el médico es el único miembro de la sociedad que puede ayudar a un paciente. Citando un caso real, un paciente acude a su médico para consultarle que sufre de paidofilia y pedirle ayuda en su lucha con su problema, y le comunica que ha llegado a rondar un colegio local temiendo no poder controlarse. El tacto de este profesional y su capacidad para convivir con su propia intranquilidad e incertidumbre consiguió llevar al paciente a manos de una buena unidad de salud mental y, finalmente, a la colaboración de miembros selectos de la fuerza pública por petición del propio paciente. Esta situación puede dar una idea de la importancia de garantizar la confidencialidad de un registro médico, independientemente de cuál sea su soporte.

COMPLEMENTOS DEL ANEXO SOBRE CONFIDENCIALIDAD

1. Folleto informativo para el paciente. Assistance Publique -Hôpitaux de Paris «Informatique & Libertés».
Dans le cadre du Systeme d´information Hospitalier (SIH) des logiciels ont été mis en place afin d´assurer la gestion du patient a l´Assistance Publique-Hôpitaux de Paris.
Ces logiciels ont reçu l´agrément de la Commission Nationale de l´informatique et des Libertés (CNIL). Ils ont pour but:
– De faciliter votre identification par les différents services de I´hôpital.
– De simplifier...
[...]
Les informations nominatives que vous nous fournissez sont enregistrées. Un numéro d´identification permanent vous est attribué, dès votre première venue à l´hôpital.
Utilisé par les applications informatiques de l´hôpital, il permet:
– D´assurer le lien entre toutes les données informatisées.
– De retrouver ces données et...
[...]
Toutes les dispositions ont été prises pour garantir la confidentialité et la protection des données saisies et traitées par les systemes (art. 378 du Code Pénal et Code de Déontologie Médicale).
Conformément à la loi n º 78.17 du 6/01/78 «Informatique et Libertés», vous disposez d´un droit d´accès et de rectification de vos informations (art. 34 à 40).
A l´issue du regrement des frais de séjour, vous pouvez obtenir, sur demande motivée, que l´acces aux données relatives a votre séjour soit anonyme. En cas d´acceptation de la demande, un numéro permanent anonyme vous sera comuniqué et deviendra, sous votre responsabilité, l´unique clé d´acces a votre dossier: vous en serez le seul possesseur.

Bien entendu, en cas de perte de ce numéro, nous ne pourrons plus retrouver la trace de ces informations.

Ces droits s´exercent sur simple demande écrite auprés du Directeur-Adjoint chargé des Affaires Générales de l´hôpital.»
2. Constitución Española de 27 de diciembre de 1978
"Sección 1.ª De los derechos fundamentales y las libertades públicas Art.18.
1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos...»

3. Kelly G. Patient data, confidentiality, and electronics. Editorials. BMJ 1998; 316: 718-719 (7 de marzo): «[...] clinicians are ultimately responsible for the safety of the patient data they commit to electronic transfer or storage [...]».
4. The Caldicott Committee. Report on the review of patient-identifiable information-December 1997: «[...] Summary of Recommendations
Recommendation 1: Every dataflow, current or proposed, should be tested against basic principles of good practice. Continuing flows should be re-tested regularly.
Recommendation 2: A programme of work should be established to reinforce awareness of confidentiality and information security requirements amongst all staff within the NHS.
Recommendation 3: A senior person, preferably a health professional, should be nominated in each health organisation to act as a guardian, responsible for safeguarding the confidentiality of patient information.
Recommendation 4: Clear guidance should be provided for those individuals/bodies responsible for approving uses of patient-identifiable information.
Recommendation 5: Protocols should be developed to protect the exchange of patient-identifiable information between NHS and non-NHS bodies.
Recommendation 6: The identity of those responsible for monitoring the sharing and transfer of information within agreed local protocols should be dearly communicated.
Recommendation 7: An accreditation system which recognises those organisations following good practice with respect to confidentiality should be considered.
Recommendation 8: The NHS number should replace other identifiers wherever practicable, taking account of the consequences of errors and particular requirements for other specific identifiers.
Recommendation 9: Strict protocols should define who is authorised to gain access to patient identity where the NHS number or other coded identifier is used.
Recommendation 10: Where particularly sensitive information is transferred, privacy enhancing technologies (e.g. encrypting identifiers or «patient identifying information» must be explored.
Recommendation 11: Those involved in developing health information systems should ensure that best practice principles are incorporated during the design stage.
Recommendation 12: Where practicable. the internal structure and administration of databases holding patient-identifiable information should reflect the principles developed in this report.
Recommendation 13: The NHS number should replace the patients name on Items of Service Claims made by General Practitioners as soon as practically possible.
Recommendation 14: The design of new systems for the transfer of prescription data should incorporate the principles developed in this report.
Recommendation 15: Future negotiations on pay and conditions for General Practitioners should. where possible. avoid systems of payment which require patient identifying details to be transmitted.
Recommendation 16: Consideration should

be given to procedures for General Practice claims and payments which do not require patient-identifying information to be transferred. which can then be piloted.»

Published by the NHS Executive 1998.

Elementos de seguridad en la informatización de centros de salud

F.A. Alonso López

Doctor en Medicina y Cirugía. Especialista en *Medicina Familiar* y *Comunitaria.*

Si entendemos por seguridad, como propuso el National Research Council en 1991, *la protección de los sistemas de información contra el acceso no autorizado y la modificación de la información, bien durante su almacenamiento, proceso o tránsito y asimismo la autorización de acceso a aquellos individuos autorizados incluyendo medidas para detectar, controlar y contabilizar tales eventos,* a nadie se le escapa que éste será uno de los puntos esenciales tanto en el desarrollo como en la posterior evaluación de sistemas informáticos para el registro de datos de pacientes.

Un sistema informático que almacene, maneje o difunda información tan sensible como la sanitaria debe tener la capacidad de ofrecer la seguridad necesaria que garantice la integridad y la confidencialidad de dicha información, a fin de proteger tanto derechos fundamentales de las personas como otros intereses legales de éstas, de los prestatarios de los servicios y de las organizaciones públicas o privadas responsables del cuidado de la salud.

En el estado actual de desarrollo de las tecnologías de la información y de los sistemas informatizados de archivo, cuando éstos cuentan en su diseño e implementación con elementos apropiados de seguridad, puede afirmarse, sin lugar a dudas, que proporcionan mayor nivel de protección para la confidencialidad e integridad de los datos de un paciente individual, que aquellos basados en archivos de papel. Sin embargo, extender tal afirmación a la confidencialidad y privacidad de datos colectivos es, cuando menos, arriesgado y exige a las organizaciones precaución extrema en los conceptos de diseño, mantenimiento y control de accesos de las aplicaciones a instaurar.

Los sistemas basados en tecnologías de la información están sometidos a una variedad de riesgos/amenazas que pueden ser clasificadas de muchas formas, tales como accidentales o deliberadas, como internas o externas, como físicas o lógicas.

Los riesgos físicos incluyen peligros ambientales, que usualmente afectan a la disponibilidad del sistema y normalmente están causados por fenómenos naturales. También incluyen peligros por intrusismo de personal no autorizado.

Los riesgos lógicos ocurren cuando los datos son alterados en alguna forma o cuando el software es alterado con perjuicio para los mismos. Estos riesgos pueden ocurrir bien deliberada o bien fortuitamente. Los riesgos deliberados gozan de gran predicamento publicitario, pero los accidentales o fortuitos son mucho más comunes.

Podemos definir una serie de ítems generales que agrupan los contenidos necesarios para considerar seguro un sistema:

Acreditación: Está en relación con la garantía de que un sujeto (acreditación de usuario} u objeto (acreditación de las fuentes de datos) es lo que dice ser.

Autorización: Es la concesión de derechos en los accesos de un individuo previamente acreditado. La autorización afecta tanto a aspectos físicos (conectarse) como lógicos (usar recursos hasta un determinado nivel).

Integridad: Propiedad por la cual la información es cambiada sólo de una forma específica y autorizada. Considerar seguro un sistema exige integridad en los datos, en los programas y en el entorno de la red en la que trabaja.

Capacidad de auditoría: Toda actividad del sistema es recogida de forma concurrente a su realización, de manera que pueda reconstruirse en cualquier momento la secuencia de eventos que condujeron a un determinado registro.

Prevención de desastres: Capacidad de recuperación de datos en casos de desastres naturales o provocados (incendios, inundaciones, hurto, vandalismo...).

Almacenamiento y transmisión: Se refiere a la localización física de los datos (almacenamiento) y a la capacidad de intercambio de los mismos cuando emisor y receptor se encuentran en lugares distintos (transmisión).

Siguiendo esta secuencia, el presente documento muestra a continuación, más que un análisis exhaustivo del tema, una guía o boceto para aquellos interesados en el desarrollo, implantación, compra o uso de este tipo de sistemas. Esta guía es un resumen que no implica en modo alguno priorización y, lógicamente, habrá de adaptarse a las circunstancias o necesidades particulares.

Requisitos exigibles de seguridad

– Existencia de código de identificación y contraseña de usuario que verifiquen el acceso al sistema.
– Dispositivos de acreditación adicionales (firmas seguras, huella dactilar), para acceso al sistema o a lugares específicos.
– Cada persona es identificada de forma individual.
– La elección de contraseña es privada sin necesidad de intervención de un administrador de sistema.
– Las contraseñas caducan, exigiendo al usuario nueva definición.
– Las contraseñas siguen unas normas claras en cuanto a su tamaño y formato de datos.
– El sistema permite que el personal de mantenimiento y soporte no acceda a datos de pacientes.
– Capacidad de detección de fecha y hora a la que se accedió por última vez con una determinada contraseña.
– Existencia de herramientas de diseño de informes de seguridad a disposición de los administradores del sistema.
– El sistema permite la definición, a nivel de usuario, de aquellos elementos funciones, comandos o menús a los que dicho usuario tendrá acceso, en función de las responsabilidades del mismo.
– Podrán diseñarse niveles de usuario agrupados.
– Los datos sensibles podrán ser encriptados, bien para su almacenamiento, bien para su transmisión.
– El usuario podrá deshabilitar opciones de visualización o impresión de datos concretos.
– Deberá poder determinarse quién y cuando accedió, o está accediendo (*on-line*) a los datos de un paciente.
– Existen herramientas que aseguran que el almacenaje de datos respeta la integridad de los mismos.

– El sistema contiene elementos que facilitan la recogida de información de forma no redundante.
– Queda constancia de las transacciones aceptadas o rechazadas y la causa.
– Existe control sobre las actualizaciones simultáneas de idéntica información. Existen barreras de acceso a través de conexión periférica o externa (disqueteras, teléfono, Internet) a modo de antivirus, cortafuegos, encriptación y sistemas de acreditación.
– Pueden definirse alarmas inmediatas ante eventos predefinidos.
– Puede auditarse quién, cuándo, dónde y sobre qué información se realizó una operación de introducción, cambio, borrado o visualización.
– Los sistemas de auditoría no podrán ser modificados por los usuarios.
– El sistema deberá soportar auditorías externas.
– Se implementarán procesos de copia dinámicos que permitan realización mientras el sistema está operativo.
– Los procesos de copia podrán automatizarse en cualquier caso.
– Existirán procedimientos y software para recuperación de datos que permitan la misma a pesar de fallos del sistema.
– Los datos se guardaran con sistemas de copia *on-line* (espejo).
– Existe control sobre importación y exportación de datos.
– El entorno de comunicaciones es estándar no precisando que el interlocutor remoto disponga de idéntica solución.
– Ante acceso remoto podrá definirse nivel del mismo, duración de la conexión, información visualizable e información exportable.
– La localización, seguridad eléctrica y aislamiento de los equipos, o al menos del servidor de datos, estará específicamente controlada.

Cultura de seguridad

Y, sin embargo, constatamos cómo, a pesar de haber exigido a fabricantes e instaladores de hard y soft, estas características anteriormente descritas, nuestros sistemas continúan siendo extraordinariamente inseguros.
Básicamente esto sucede porque hemos olvidado exigirnos a nosotros mismos, sus usuarios, la capacidad de poner en práctica la seguridad del sistema que exigimos a los demás.
Por eso no es infrecuente, a nada que uno se pasee por centros de salud informatizados, encontrar ordenadores encendidos en consultas donde no hay nadie, áreas administrativas en las que todo el mundo ingresa con claves de acceso intercambiables y que, para remate, se encuentran pegadas con un *post-it* en el monitor. Situaciones trágicas en las que un error de disco pierde todas las historias clínicas porque no hay copias de seguridad actualizadas, o se restaura una copia de seguridad incorrectamente etiquetada, dando por buenos datos anticuados, etc.
Podríamos definir, también a modo de boceto, una serie de requisitos exigibles a un centro en lo referente a su cultura interna de seguridad:

– Definición nominal de responsable de seguridad del sistema y tareas asignadas a él (auditoría y revisión periódica de cultura de seguridad entre el personal).
– Definición nominal de responsable de realización y archivado de copias de seguridad.
– Existencia de lugar específico y adecuado de almacenaje en el centro (armarios resistentes al calor) y fuera de él (evitación del desastre total como incendio, inundación...).
– Las copias son registradas y etiquetadas para su almacenaje.
– Definición de copias cíclicas (alternas y semanales por ejemplo).
– Restauración periódica de copias para revisar integridad.
– Cambio periódico de soporte físico (al menos una vez al año se adquieren nuevos soportes).

Relación primaria-especializada

Luis Sánchez Perruca. Médico de Familia. Responsable de Tecnologías y Sistemas. Área 8 *de Atención Primaria. Madrid.*

Introducción

La evolución del conocimiento y de la tecnología, la forma de organizar y financiar los servicios sanitarios, dibujan los límites de la atención primaria, la atención especializada y la atención sociosanitaria[1].
Los avances científicos y diagnósticos han desplazado en ocasiones la divisoria en la prestación de la atención sanitaria, siendo la variable clave la capacidad resolutiva de cada nivel, estando influenciada esta última por variables epidemiológicas.
El enfoque integral hacia el paciente exige coordinación importante en el proceso de atención mediante la cooperación de los distintos niveles asistenciales en las que cada actor asume su papel en un continuo asistencial.
La introducción de la competencia entre niveles, entendida como un instrumento al servicio de la eficiencia y no como un intento mutuo de derivarse las responsabilidades, redundará en una mejora de la atención al usuario.
No olvidemos que cooperación significa aunar esfuerzos para alcanzar un mismo fin.
Si en el contexto descrito nos movemos con naturalidad, a nadie se le puede escapar que los diferentes niveles no serán cada uno un mero filtro del siguiente, sino que los niveles asistenciales formarán parte del todo que es la organización sanitaria y que, además, tienen un objetivo común: el cuidado del individuo y su entorno[2].
El patrón epidemiológico y la conjugación de los criterios de efectividad, satisfacción y costes han de ser quienes determinen la configuración de la organización sanitaria en niveles asistenciales, estableciendo entre ellos al mismo tiempo la competencia, así como su capacidad resolutiva[3].
Teniendo en cuenta que estamos en un momento de oportunidad de cambio, junto al empuje en el desarrollo de herramientas cada vez mejor orientadas a la automatización de los sistemas de información sanitarios, se añade un elemento definitivo en la resolución de esta falta de comunicación, y son las redes de transmisión de datos que ya son una realidad en nuestro ámbito de actuación.
Por todo ello, en este momento la dificultad de coordinación entre los niveles asistenciales primaria y especializada se nos antoja como sinfonía inacabada difícil de sostener en la realidad actual de cara a los usuarios de los servicios sanitarios. Éstos nos demandan la obligación de «ponernos de acuerdo» en los procedimientos funcionales que hagan posible la comunicación real entre ambos niveles.

Bases conceptuales en la relación primaria-especializada[4]

– El papel de la atención primaria como puerta de entrada al sistema

sanitario del paciente. Garantiza la entrada al mismo y la coordinación de su proceso de atención, dado que es ésta la que le dota de una visión integral y longitudinal en el tiempo.
– El papel de la atención especializada como nivel complementario en la resolución de problemas.
– Garantía de continuidad de la atención, de manera que no se produzca ninguna ruptura sea el nivel donde resida la asistencia en un determinado momento del relato patográfico del paciente.
– Orientación del sistema hacia el paciente, usuario, ciudadano.
– Las nuevas tecnologías de la información, como herramientas. En este contexto, la introducción las nuevas tecnologías de la información representa una doble oportunidad:
1. General, en cuanto a que cualquier elemento nuevo debe ser motivo para revisar y replantear conceptos y formas de actuar.
2. Específica, por lo que pueden aportar como herramientas al servicio de los profesionales, de la población y de la organización.
– Mantener la propia evolución e independencia organizativa en ambos niveles, junto a las herramientas tecnológicas que lo desarrollan. Ello obliga a un diseño flexible y evolutivo donde debe prevalecer el aspecto funcional como elemento más adaptable a los cambios de realidades y necesidades.
– Siempre debemos de tener presente que una excelente herramienta informática, aun cumpliendo estrictamente las reglas de estandarización y conectividad, será una herramienta inútil si no se crea con unas bases sólidas de participación de los profesionales que las usen, y no cumplan los objetivos funcionales para lo que han sido desarrolladas.

Áreas de actuación

Uno de los acontecimientos que más han empujado a que se esté hablando ahora de la conexión entre los hospitales y/o ambulatorios de especialidades con los centros de atención primaria es que hayamos superado la barrera técnica de la comunicación informática. En los últimos tiempos, de forma habitual, se ponen en marcha proyectos utilizando las redes de comunicación existentes: abiertas, como Internet, y restringidas, como las Intranet corporativas.

Cuando nos referimos al ámbito de la telemática, en los servicios sanitarios nos encontramos con el término acuñado hace tiempo de «telemedicina»; este amplio concepto incluye un abanico de actuaciones, con diferentes realidades prácticas según su aplicación.
Es de sentido común que abordemos aquí unos aspectos realizables y de principal interés de abordaje, como son:

– Gestión bidireccional de la demanda entre atención primaria y atención especializada.
– Intercambio de información electrónica.
– Acceso a la historia clínica del paciente.

Y otros aspectos de la comunicación entre niveles asistenciales que deberán ser consecuencia de validaciones exhaustivas pertinentes de su eficiencia, cuya consecución no cabe duda de que debe ser objetivado en su consecución. A más largo plazo:

– Telerradiología.
– Teleconsulta y telediagnóstico.

Sería un error derivado de los defectos actuales de compartimentalización de tareas tratar estos aspectos sin pensar en el dimensionamiento funcional de la integración de algunos de ellos.

Gestión bidireccional de la demanda entre atención primaria y atención especializada. Intercambio de información electrónica (documentos de interconsulta)

La gestión de derivaciones entre atención primaria y especializada es un elemento clave para la optimización de la accesibilidad y fluidez del paciente dentro del sistema sanitario.
En la actualidad, tanto la gestión de las agendas como de la demanda dependen exclusivamente de atención especializada, quien asigna la cita en función de parámetros administrativos y asistenciales propios. Al carecer atención primaria de la oportuna información sobre las demoras en la atención, ésta queda relegada al papel de simple emisor de interconsultas.
Todos los procesos quedan supeditados al «cuello de botella» de la rigidez de este sistema administrativo. provocándose numerosos cortes en el proceso asistencial del paciente.
El análisis del circuito de derivaciones actual nos permite determinar los problemas de partida:
– Derivados del soporte documental y su vehiculización.
– La manipulación de los partes de derivaciones pueden conducir a extravíos o mala clasificación de los mismos con las citaciones, además de producir un coste administrativo importante.
– Derivados de la documentación escrita. La transcripción de datos muchas veces son ilegibles y los datos administrativos incompletos.
– Derivados de la falta de participación del paciente en su proceso de atención. El paciente en muchas ocasiones es un mero receptor de información, no participando en la elección de la cita más adecuada a sus necesidades, generándose en un porcentaje nada desdeñable un cambio de cita, y lo que es más importante, anulaciones de hecho sin que el sistema pueda detectarlas y reutilizar estos recursos de forma adecuada.

Existen experiencias próximas con resultados dispares donde se ha enfocado el problema como meramente administrativo. El simple cambio de tareas administrativas que sólo implique el lugar donde se cite quedaría lejos de pretender el inicio de una comunicación real entre ambos niveles.
La implantación de una interconsulta desde un nivel a otro en tiempo real debe tener muy claros sus objetivos de mejora de la situación actual. Estos objetivos establecidos en beneficios o impactos positivos deben beneficiar a todos los actores implicados en el circuito:

Sobre la población

– Obtener cita inmediata a la consulta de atención primaria y desde la propia unidad administrativa del centro.
– Disminuir las molestias debidas a fallos de coordinación y pérdidas de información.
– Mejorar los tiempos en la resolución de los problemas de salud y en los trámites administrativos.
– Disminuir los olvidos y ausencias a las citas por parte del paciente.
– Posibilidad de elegir día, hora y especialista.

Sobre los profesionales

– Disminuir cargas y trámites administrativos.
– Garantizar el acceso inmediato a la información del otro nivel de atención.
– Mejorar la fiabilidad en la transmisión y circulación de la información (pérdidas y duplicidades).
– Mejorar la comunicación entre profesionales.
– Facilitar una mejor coordinación clínica y terapéutica.
– Disminuir la necesidad de transcripción de información
– Capacidad de gestionar la cita directamente sobre la agenda del especialista (saber a tiempo real cuándo el especialista atenderá al paciente).
– Mejorar la gestión de las agendas propias (cita anticipada del paciente en función de la visita al especialista).
– Conocer en cada momento las listas de espera.
– Facilitar la comunicación al alta de atención especializada a atención primaria.
– Mejorar la satisfacción de los profesionales.

Sobre la organización

– Mejor gestión de las listas de espera.
– Mayor fiabilidad del sistema de información.
– Optimización de procesos y de los recursos tecnológicos.

Objetivos técnicos

– Diseñar las especificaciones funcionales de un modelo de comunicación/transacción informática entre niveles estándar sean cuales sean las aplicaciones informáticas implantadas.

Objetivos económicos

– Evitar los costes debidos a ineficiencias del sistema actual (duplicidad de exploraciones, segundas citas por errores en la comunicación, prolongaciones innecesarias de procesos de IT por fallos y demoras en los circuitos de citación, etc.).
– Cuantificar y desagregar el coste de la compra de servicios entre niveles.
– Facilitar la evaluación de costes y de procesos.

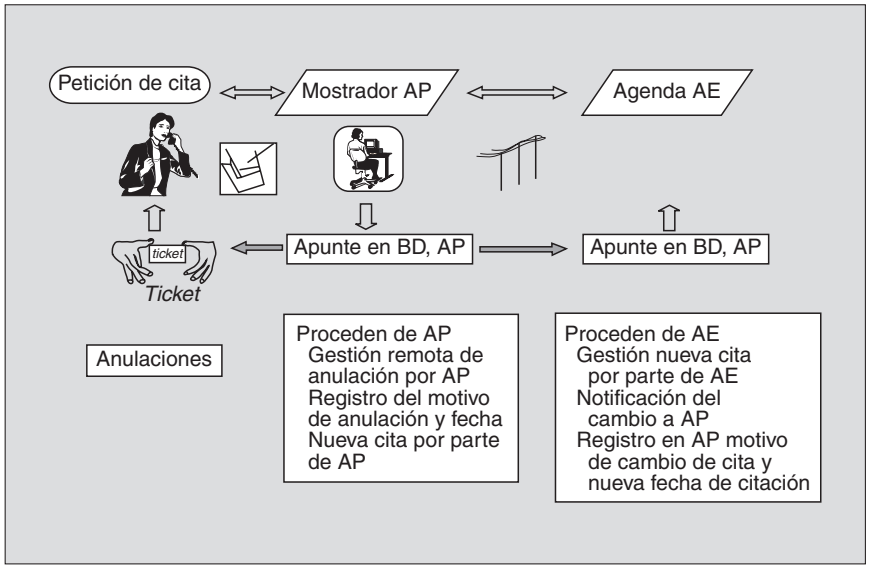

Figura 1.

Propuesta de modelo

El sistema propuesto representa un cambio radical con el sistema actual. Se basa en la asunción conjunta de riesgos entre atención primaria y atención especializada mediante la gestión de las agendas por parte de atención especializada y de la gestión de la demanda generada por parte de atención primaria.
Gestionar las agendas significa proveer de consultas a las necesidades generadas por atención primaria, con la antelación suficiente que permita mantener una lista de espera adecuada, al tiempo que resuelve la necesidad de consultas internas generadas por la propia atención especializada.
Esto sólo es posible en un marco de compra de servicios y de mutua confianza entre ambos niveles asistenciales.
No nos referimos con la definición de las distintas agendas por especialidades y médico, aspecto éste previo a la gestión, sino a la provisión de consultas acordes con la demanda, junto con los mecanismos necesarios de control.
Gestionar la demanda significa asignar la consulta en función de diferentes parámetros clínicos y de gestión, ajustándola con los acuerdos firmados con atención especializada y a los estándares de calidad prefijados para la especialidad, asumiendo riesgos y beneficios conjuntamente.
Los acuerdos deben fijar cartera de servicios de cada una de las especialidades, presión diaria de nuevas consultas, límite máximo de demora en las distintas especialidades y los mecanismos de disminución y control de las listas de espera.
Términos como proceso, primera consulta, consulta normal, urgente o preferente, deben quedar explícitamente definidos y acordados por ambos niveles asistenciales.

Modelo de circuito automatizado

Las herramientas informáticas implantadas en atención primaria estarán dotadas internamente de un circuito de gestión y generación de partes de interconsulta automatizados, con el fin de preparar la información necesaria de origen para su envío por vía telemática (fig. 1).

– En la herramienta informática del centro de atención primaria se adecuará la información recogida de la generación del parte de interconsulta generado por el facultativo y unirá a los datos de identificación del paciente necesarios para su identificación dentro del circuito.
– El proceso de enlace con la petición de citación con la herramienta informática de atención especializada se realizará de forma transparente para la unidad administrativa del centro de atención primaria e integrada desde dicha herramienta.
– Todos los procesos de control cumplirán los estándares de comunica-

ción y mensajes de control y flujo normalizados.
– Una vez establecida la conexión con la base de datos de citación de atención especializada, la unidad administrativa del centro de atención primaria oferta al paciente las posibles citas disponibles a partir de los criterios de petición indicados por el propio paciente.
– Cuando la elección de la cita sea confirmada, el sistema construirá un código de proceso unívoco que servirá como identificador de los documentos anexos que serán enviados vía telemática a disposición de atención especializada.
– La confirmación de la conclusión del proceso de citación vendrá dado por la emisión de un ticket recordatorio de la citación, que será entregado al paciente en la unidad administrativa del centro de atención primaria.
– El registro de citación del paciente quedará reflejado en la herramienta informática de atención primaria, integrada en ella como si de una cita interna se tratara.
– El médico de atención primaria, a través de la herramienta informática, tendrá notificación de la citación a atención especializada en su gestión interna de la historia del paciente pendiente de la recepción de respuesta.
– Los cambios y anulaciones de citación se realizarán según la siguiente norma:

a) Cambios y anulaciones por parte del paciente. Se realizarán en el lugar donde el paciente acuda para su realización, habitualmente por su mejor accesibilidad lo realizará en el centro de atención primaria.
b) Cambios y anulaciones por ajuste de agendas. Se realizará por parte de la UADE. En este caso atención primaria recibirá notificación con un proceso automático de cambio de citas en su propia herramienta informática.
c) En el caso de anulaciones por parte del propio paciente, el médico recibirá información en su historia clínica informatizada, como respuesta a su interconsulta.
d) La elaboración de la respuesta a la interconsulta por parte del facultativo de atención especializada se elaborará en la herramienta habitual de trabajo de éste.
e) La vehiculización del documento hacia atención primaria se llevará a cabo a través de estándares de comunicación telemática, cuya identificación unívoca vendrá dada por el código de proceso generado en la confirmación de cita dada previamente desde atención primaria.
f) A través de un circuito interno de actualización, dicho documento se anexará de forma automatizada en la historia clínica del centro de atención primaria, identificándolo el médico con su propia herramienta de gestión clínica.

Funcionalidades internas de la herramienta informática de comunicación

– Los actores implicados en el circuito deberán estar identificados en todo momento, de tal forma que cualquier actuación por su parte deje un rastro en el sistema, tanto en la herramienta de atención primaria, como de atención especializada.
– El sistema deberá cumplir los estándares de seguridad establecidos (véase anexo de seguridad) en cuanto a:
a) Acceso, restricciones y vulnerabilidad.
b) Integridad de la información y su circulación. Elaboración de la información transferible en formatos estándar de exportación e importación de datos.
c) Protección de datos de una forma específica en el sistema de mensajería electrónica que vehicule los documentos anexos, con los protocolos de actuación ante datos sensibles (normalización de encriptación y de datos mínimos de identificación de proceso).
– La herramienta de conexión deberá incluir en su desarrollo elementos de control de flujo, para la identificación y notificación a los actores de las transacciones erróneas por una ausencia de comunicación en el proceso de interconexión.

Otras funcionalidades

El centro de atención primaria deberá disponer de información suficiente para que el paciente disponga de la mejor accesibilidad al sistema:
– Información de la lista de espera de la especialidad que solicita la citación.
– Información necesaria sobre las agendas de las distintas especialidades.
– Por otra parte, deberá disponer de un sistema de explotación para la gestión de sus propias derivaciones.

Intercambio de información electrónica (circuito de automatización de pruebas de laboratorio)

Junto con la gestión de las derivaciones, uno de los elementos de la consulta diaria de atención primaria más «rentables» que debemos abordar es la automatización de los resultados de pruebas de laboratorio.

Objetivos específicos

– Generación de la petición de analítica automatizada.
– Recogida automatizada del resumen de muestras a tomar por parte del laboratorio identificación, envío y recepción de resultados en el propio centro.
– Control de gestión de peticiones realizadas, e identificación de los motivos de pérdida en la entrada del circuito.
– Control y gestión de la situación de las pruebas en cualquier punto del circuito.
– Evitar repetición de pruebas por errores del circuito actual.
– Optimización en el seguimiento del paciente en su proceso de atención.

Circuito de pruebas de laboratorio

– La herramienta informática de atención primaria realizará la gestión interna del circuito de petición de pruebas de laboratorio.
– Se establecerá una conexión no en tiempo real y a determinar en la temporalidad con el objetivo de la unificación del catálogo de pruebas de determinación del laboratorio de referencia.
– El circuito se realiza según se muestra en la figura 2.
– En la herramienta informática del centro de atención primaria el facultativo realizará las anotaciones correspondientes a las peticiones de pruebas de laboratorio, además de la información complementaria especifica necesaria para la adecuada realización y análisis de las mismas.
– En la unidad de extracciones del centro de atención primaria, se completará la información necesaria de identificación de muestras, así como la identificación del proceso en la

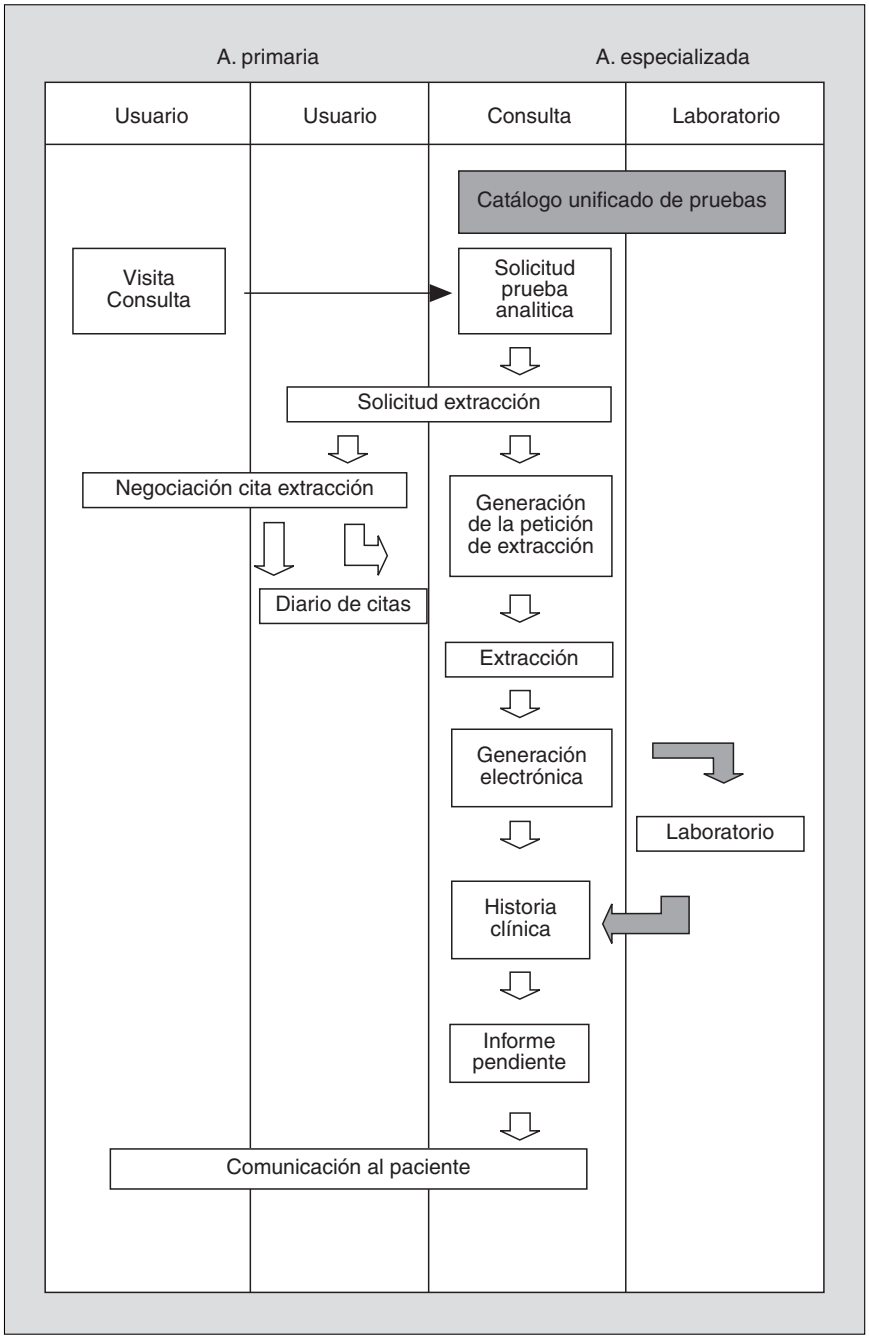

Figura 2.

una herramienta de gestión de pruebas de laboratorio que esté enlazada con la historia clínica informatizada del centro.
– Construcción de un fichero de datos con la petición de análisis de pruebas, que previamente se haya diseñado para la transacción electrónica de los mismos (datos de identificación de usuario y muestras incluidas en el proceso, además de la codificación de cada una de las pruebas e informe asociado a la petición).
– Comunicación con el laboratorio para el envío del fichero de petición. En ese momento en la herramienta del centro de atención primaria y en su programa de gestión se integra el código de las muestras incluidas en el proceso en espera de resultados.
– Validación del fichero de peticiones por parte de la herramienta informática del laboratorio y emisión de un mensaje de conformidad al centro de atención primaria.
– Envío de las muestras incluidas en el proceso.
– El análisis de las muestras enlazará en su herramienta informática con el fichero de identificación de las mismas que desde atención primaria se ha remitido.
– El laboratorio elabora un fichero de resultados, cuyo formato ha sido diseñado y adecuado a la transacción electrónica, y es puesto a disposición de envío a través de una herramienta informática de mensajería electrónica. Este fichero de resultados deberá incluir en su contenido los valores de referencia de dicha prueba.
– La herramienta informática del centro de atención primaria analizará los resultados enviados frente a las peticiones emitidas, informando a éste el grado de realización de las mismas, indicando el cierre del proceso de recepción de resultados cuando se complete la petición de origen.
– La herramienta informática del centro de atención primaria se encarga en un proceso automatizado de insertar los resultados en la historia clínica del paciente, y su programa de gestión deberá indicar al facultativo del centro la disponibilidad de resultados.
– Al igual que en el apartado anterior (gestión bidireccional de la demanda), deberá cumplir las funcionalidades internas de comunicación que allí fueron mencionadas.

Acceso a la historia clínica

Cuando hablamos del acceso a la historia clínica, necesariamente lo primero que nos debemos de cuestionar es: ¿qué información debemos de conocer en el ámbito sanitario de un paciente ante una actuación básica en salud?, independiente del nivel de atención en el que nos situemos.
Ante esta necesidad, claramente debemos poner unos límites; éstos deben seguir la línea descrita en el documento general que acompaña a este anexo donde se establece que «el sistema de información debe garantizar a los pacientes que los profesionales responsables de su cuidado podrán acceder, de manera rápida y fiable, a la información clínica personal necesaria para el cuidado de su salud, respetando su confidencialidad».
Al mismo tiempo, tenemos que ser conscientes de que partimos de dos

realidades asistenciales funcionalmente diferentes y con un desarrollo automatizado de la información adaptado a cada necesidad (atención longitudinal y transversal en el proceso asistencial del paciente).
Teniendo en cuenta lo expresado, debemos de avanzar en la opción de información compartida ante la opción de información unificada.

Directrices funcionales

– Los profesionales asistenciales deberán definir de forma consensuada aquella información útil que es generada por el estamento complementario de atención sanitaria, con el compromiso firme de mantener en perfecta actualización por cada uno de los niveles asistenciales aquella información básica susceptible de compartir.
– La plataforma tecnológica definirá el conjunto de elementos, herramientas y protocolos que permitan integrar el conjunto de datos básicos de la biografía sanitaria del paciente, así como de definir los niveles de seguridad de acceso a la información, garantizando su confidencialidad (este punto se desarrolla con amplitud en los anexos de seguridad y conjunto mínimo de datos, que acompaña al documento general).
Algunos de los aspectos anteriormente contemplados ya están siendo objeto de validación en sus circuitos de acceso y en su integración con la historia clínica de atención primaria, como son el seguimiento de hospitalización e información generada en el alta hospitalaria y en la información asimismo suministrada por servicios de urgencia hospitalarios.

Teleconsulta (telerradiología, telediagnóstico)

Uno de los elementos más buscado por la sociedad de la información en nuestros días es la comunicación en tiempo real (audio y videoconferencia). El mundo comercial y educativo se está haciendo eco de una forma evidente de estas «nuevas» herramientas.
Los elementos clave que favorecen esta evolución serían:

– El uso cada vez mayor de Internet y su potencial está haciendo que las herramientas multimedias sean mejoradas día a día.
– El gran avance que ha supuesto las herramientas de compresión real de la imagen y el sonido, con una calidad cada vez mas evidente.
– La inclusión de nuevos protocolos de comunicación en tiempo real que permiten identificar tanto las fuentes emisoras, como el contenido de los datos que viajan por las redes de comunicación, para determinar el tipo de codificación y decodificación que hay que aplicarles.
– Las líneas de comunicación de alta velocidad basadas en fibra óptica, que permiten enviar una mayor información cada vez en menor tiempo.

El entorno sanitario cada vez más se está haciendo más eco de esta nueva forma de comunicación, y es ahora donde se comienzan a realizar experiencias en este campo.
En un futuro no lejano la relación entre niveles asistenciales deberá adoptar e integrar estas herramientas de videoconferencia como un elemento básico funcional en sus desarrollos de gestión de la historia clínica informatizada.
Si hemos desarrollado en puntos anteriores de este anexo la integración de datos de laboratorio y documentación clínica dentro de la historia clínica como aspectos importantes para la relación entre niveles asistenciales, la digitalización de imágenes de pruebas complementarias (radiología en especial) sería el siguiente punto que deberíamos integrar en ella.

¿Cuál es el paso que nos falta para aceptar la validez de estas herramientas?:

– Asumir que el ámbito sanitario debe ofrecer servicios al usuario que ya están empezando a ser habituales en su entorno.
– Además de normalizar y estandarizar estas herramientas, lo cual lleva tiempo haciéndose, el profesional sanitario debe adecuar su forma de trabajo para incluirlas en su trabajo habitual.
– Establecer claramente el coste-efectividad de estas nuevas tecnologías y su rentabilidad.
– La implicación de los profesionales sanitarios en la validez interna de estas herramientas como ayuda diagnóstica en su actuación clínica diaria.

Agradecimientos

A los médicos de familia J. Custodi i Canosa y J. Pérez Ramírez, por su aportación al diseño conceptual y funcional de los modelos propuestos en este anexo.

Bibliografía

1. Ortún Rubio V. La articulación entre niveles asistenciales. En: Llano Señarís J, Ortún Rubio V et al. Gestión sanitaria. Innovaciones y desafíos. Barcelona: Masson, 1998; 349-357.
2. Aranaz Andrés JM, Buil Aina JA. Gestión sanitaria: acerca de la coordinación de niveles asistenciales. Med Clin (Barc) 1993; 106: 182-184.
3. Ortún Rubio V. Clínica y gestión. Med Clin (Barc) 1995; 104: 298-300.
4. Custodi J, Pérez J, Sánchez L. Bases conceptuales y análisis funcional de la gestión bidireccional de la demanda entre el hospital y atención primaria. (Documento interno-Anexo Proyecto Sinfal «Sistema de Información Asistencial Integrado para el Area de Alcorcón»). Octubre, 1998.