Datuak Babesteko
Euskal Bulegoa

Agencia Vasca de
Protección de Datos

**CN13-049**

# DICTAMEN RELATIVO A LA CONSULTA PLANTEADA POR EL DEPARTAMENTO DE SANIDAD DEL GOBIERNO VASCO RELATIVA A LOS ACCESOS A LAS HISTORIAS CLÍNICAS DE OSAKIDETZA-SERVICIO VASCO DE SALUD POR PARTE DEL PERSONAL SANITARIO DE RESIDENCIAS Y CENTROS DE DÍA.

## ANTECEDENTES

**PRIMERO:** Con fecha 28 de noviembre de 2013 se ha formulado consulta ante la Agencia Vasca de Protección de Datos en relación con el asunto arriba referenciado.

**SEGUNDO:** El artículo 17.1 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, en su apartado n) atribuye a la Agencia Vasca de Protección de Datos la siguiente función:

> *"Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones a que se refiere el artículo 2.1 de esta Ley, así como otras personas físicas o jurídicas, en relación con los tratamientos de datos de carácter personal incluidos en el ámbito de aplicación de esta Ley."*

Corresponde a esta Agencia Vasca de Protección de Datos, en virtud de la normativa más arriba citada, la emisión del informe en respuesta a la consulta formulada.

La entidad consultante ha manifestado verbalmente la urgencia en la emisión de este Dictamen, y esta Agencia, siendo sensible a esta petición, ha procurado emitirlo en el plazo más breve posible. Esta urgencia provoca por otra parte no poder entrar a resolver todos los supuestos planteados por el Departamento de Salud, y tener que limitarnos a resolver el planteamiento general del marco relacional entre la entidad Osakidetza y las residencias o centros de día, y el acceso a la historia clínica de los pacientes que se encuentran en dichos centros por el personal al servicio de los mismos, desde una resolución general de los problemas que en perspectiva de protección de datos personales se plantean en este ámbito. Asimismo, y como se verá en el informe, se ha intentado por esta Agencia dar solución en clave positiva a una problemática que claramente es comprendida y asumida desde esta Institución, pero que por otra parte se ve constreñida por la regulación actual. Es desde la comprensión del problema existente como debe ser asumida esta consulta y en esta perspectiva hemos actuado.

Es voluntad de esta Agencia resolver posteriormente, en colaboración permanente con la entidad consultante, mediante peticiones de dictamen específicas y reuniones de coordinación entre ambas entidades, todos y cada uno de los distintos supuestos que se

plantean y que básicamente tienen que ver con la forma jurídica de cada una de las residencias o centros de día existentes en el País Vasco, que a fecha de hoy presentan una casuística muy diferente que debe ser analizada individualmente. También tendrá que ver esta respuesta con la situación concreta de la residencia en cuanto a su financiación, es decir, si es concertada, gestionada por entidades privadas previo acuerdo o contrato con la Administración Pública, y sobre todo tendrá que ver con la relación laboral/funcionarial que tenga el médico y personal sanitario que preste servicios en la residencia o centro de día.

Así pues, en este Dictamen se realizarán reflexiones generales, que establezcan los principios generales de esta relación, sin perjuicio de la debida profundización e individualización de cada uno de los casos que se vayan implantando en el País Vasco, y posteriormente se irán analizando cada uno de los supuestos concretos a resolver en colaboración entre ambas entidades.

## CONSIDERACIONES

Se formula el presente dictamen ante la consulta formulada por el Departamento de Salud del Gobierno Vasco en relación al establecimiento de un sistema que permita el acceso a las historias clínicas de pacientes de Osakidetza-Servicio Vasco de Salud, que a su vez residen o acuden a Residencias o Centros de día.

### I

Antes de pasar al estudio de las cuestiones planteadas, se debe realizar unas consideraciones generales en torno a los datos de salud, consideraciones que serán tenidas en cuenta a la hora de resolver las cuestiones planteadas.

Es preciso establecer el marco en el que nos encontramos en este ámbito, cual es el de los datos de saludo. La especial consideración de los datos de salud no solo se refleja en nuestra normativa interna, sino en los distintos textos internacionales aplicables y vinculantes para España.

El Convenio nº 108 del Consejo de Europa de 28 de enero de 1981 establece en su artículo 6 que:

> *"Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas".*

Debe ser igualmente objeto de cita el Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la biología y la medicina, hecho en Oviedo el 4 de abril de 1997 y ratificado mediante Instrumento de 23

de julio de 1999 (BOE nº 251 de 20 de octubre de 1999) que constituye el primer instrumento internacional que trata el derecho a la información, el consentimiento informado y la intimidad de la información relativa a la salud de las personas estableciéndose un marco común para la protección de los derechos humanos y la dignidad en el campo de la biología y la medicina, configurándose en su artículo 5 como regla general para una intervención en el ámbito de la sanidad el consentimiento informado de la persona afectada.

El artículo 8.1 de la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo referente al tratamiento de los datos personales y a la libre circulación de estos datos, y en cuanto su considerando 33 reconoce que tal tipo de datos relativos a la salud constituyen *"datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad"* establece que:

> *"Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad."*

La especial protección conferida a los datos de salud por las normas internacionales y comunitarias tienen reflejo en la LOPD que establece un régimen jurídico específico contenido básicamente en el apartado **3 del artículo 7**, artículo dedicado a los "*datos especialmente protegidos"* merecedores del más alto nivel de protección por afectar a los aspectos más íntimos de la personalidad, situándose en un plano en el que confluyen dos derechos fundamentales: el de intimidad y de protección de datos de carácter personal.

De acuerdo con tal apartado:

> *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente."*

Dada la incidencia especial de los datos de salud, como datos sensibles, en la esfera íntima del afectado, la LOPD ha establecido una regulación específica y más rigurosa que la establecida con carácter general tanto en lo referente a los supuestos en que será posible el tratamiento de los datos como en lo que atañe a las medidas que habrán de adoptarse para garantizar la seguridad en el tratamiento de los datos, así como el cumplimiento de deberes de confidencialidad y sigilo que deben regir en el mencionado tratamiento, de tal manera que la necesidad de obtener el consentimiento expreso de los titulares de tales datos constituye la regla general para el tratamiento de los mismos.

No obstante, el mismo artículo 7.3 contempla la posibilidad de que dicho tratamiento pueda llevarse a cabo en los supuestos en los que una ley así lo disponga debiendo quedar dicha habilitación fundada en la existencia de razones de interés general.

Conviene profundizar en el significado de la expresión *"…solo…cuando…así lo disponga una ley".*

En tal sentido debiera comenzarse otra vez por la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

De acuerdo con el apartado 4 del artículo 8 de la misma,

> *"Siempre que dispongan las garantías adecuadas los Estados miembros podrán por motivos de interés público importantes establecer otras excepciones además de las previstas en el apartado 2 bien mediante su legislación estatal, bien por decisión de la autoridad de control."*

El Considerando 34 de la Exposición de Motivos de la Directiva 95/46/CE contiene la explicación de dicho precepto. De acuerdo con tal considerando *"se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde no obstante prever las garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas".*

Por su parte, el Grupo de Trabajo sobre protección de datos del artículo 29, en el documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los **historiales médicos electrónicos**, ha interpretado también el artículo 8.4 de la Directiva y ha entendido que

> *"En cada caso, el conjunto de tratamientos de datos objeto de excepción deberá presentar un interés público importante para el Estado miembro y dicho tratamiento deberá ser necesario a la luz de tal interés público importante. Este tipo de medidas deben ser proporcionadas es decir no deben existir otras medidas que supongan menos excepciones.*
>
> *Además para que una interferencia con el derecho a la vida privada y familiar sea legítima, deberá ser conforme con el artículo 8 del Convenio Europeo sobre Derechos Humanos y deberá entenderse a la luz de la jurisprudencia de Estrasburgo: debe hacerse de conformidad con la ley y ser necesaria en una sociedad democrática a efectos de un interés público. La jurisprudencia de Estrasburgo ha afirmado en varias ocasiones que la ley que establezca la excepción debe indicar el alcance del poder discrecional conferido a las autoridades competentes y la forma de su ejercicio con la suficiente claridad teniendo en cuenta el objetivo legítimo de la medida en cuestión, a fin de proporcionar al individuo una protección adecuada contra la arbitrariedad."*

El apartado 3 del artículo 8 de dicha Directiva proyecta la anterior previsión a los datos de salud estableciendo que:

> *"El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto."*

El punto 7, apartado primero de la Recomendación 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 trata precisamente de la comunicación de este tipo de datos,

estableciendo como regla general en cuanto a su comunicación que *"Los datos médicos no se comunicarán salvo en las condiciones establecidas en este capítulo y en el Capítulo 12."*

El apartado tercero de dicho punto, en lo que ahora más puede interesar, contempla dos supuestos en los que es posible la comunicación de dichos datos sin el consentimiento de su titular:

> *"a) cuando la comunicación esté prevista por una Ley y constituya una medida necesaria en una sociedad democrática por:*
>
> *i. razones de salud pública; o*
>
> *ii. la prevención de un peligro real o la represión de un delito específico; o*
>
> *iii. otro interés público importante; o*
>
> *iv. la protección de los derechos y libertades de otros*
>
> *b) cuando la comunicación sea permitida por una Ley con fines de:*
>
> *i. protección del sujeto de los datos o de un pariente en línea genética*
>
> *ii. salvaguarda de intereses vitales del afectado o de una tercera persona; o*
>
> *iii. el cumplimiento de obligaciones contractuales específicas; o*
>
> *iv. el establecimiento, ejercicio o defensa de una reclamación legal."*

Señalándose igualmente que:

> *"Esta excepción cubre solamente el tratamiento de datos personales para el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia y a efectos de la gestión de estos servicios sanitarios como por ejemplo facturación, contabilidad o estadísticas.*
>
> *No se cubre el tratamiento posterior que no sea necesario para la prestación directa de tales servicios, como la investigación médica, el reembolso de gastos por un seguro de enfermedad, o la interposición de demandas pecuniarias. También queda fuera del alcance de la aplicación del apartado 3 del artículo 8 otros tratamientos en áreas como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen de seguro de enfermedad, dado que éstos se mencionan en el considerando 34 de la Directiva como ejemplos para invocar el apartado 4 del artículo 8."*

Dichas previsiones comunitarias son también objeto de transposición por la LOPD.

Así, el **artículo 7.6 de dicha Ley Orgánica**, de acuerdo con el cual:

> *"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.*

*También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado está física o jurídicamente incapacitado para dar su consentimiento."*

Tal precepto ha sido objeto de interpretación por la jurisprudencia y así la Audiencia Nacional, en Sentencia de 31 de mayo de 2002 ha indicado que la excepción prevista en el artículo 7.6 **habrá de ser interpretada restrictivamente**, considerando que será preciso atender en cada caso concreto a que el tratamiento se dirija efectivamente a la prevención y el diagnóstico. En este sentido, un tratamiento para un fin distinto (en el caso analizado, el control del absentismo laboral) en que estas finalidades puedan ser consideradas "secundarias" no se encontraría amparado por lo dispuesto en la Ley Orgánica 15/1999.

Más recientemente confirma dicha estricta interpretación la **Sentencia del Tribunal Supremo de 20 de octubre de 2009** que casa una anterior de la Audiencia Nacional de 24 de mayo de 2007, y de acuerdo con la cual:

*"En cuanto a la historia clínica, es cierto que los arts. 14 y siguientes de la Ley de Autonomía del Paciente favorecen "la máxima integración posible de la documentación clínica de cada paciente" a fin de lograr una adecuada asistencia sanitaria. Tal vez ello justifique hablar, como hace la sentencia impugnada, de un principio de unidad de la historia clínica. Dicho esto, es preciso inmediatamente señalar que esa integración de la historia clínica, tendente a evitar la dispersión de la información sanitaria sobre cada paciente, tiene como beneficiario al propio paciente. El inciso inicial del art. 16 de la Ley de Autonomía del Paciente es paladinamente claro a este respecto: "La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente." Las historias clínicas no deben tener carácter unitario, como pretende la sentencia impugnada, para facilitar su misión a las mutuas de prevención de riesgos laborales, ni menos aún a los empresarios. Ciertamente, permiten prestar una asistencia sanitaria mejor; pero esta mejora no se justifica por el ahorro de esfuerzo para terceros (personal sanitario, Administración, empresarios, etc.), sino por el bienestar del paciente. Este punto es de crucial importancia, porque la información sobre la salud de las personas forma parte del objeto protegido por el derecho fundamental a la intimidad, tal como ha aclarado, entre otras, la sentencia del Tribunal Constitucional 196/2004. De aquí que toda excepción a la confidencialidad que pesa sobre dicha información sólo pueda justificarse por el beneficio que reporte al propio paciente o, en su caso, por ineludibles y superiores exigencias de interés general debidamente ponderadas, que de ningún modo pueden consistir en un funcionamiento más ágil de las mutuas de prevención de riesgos laborales. Tan es así que el art. 18 de la Ley de Autonomía del Paciente sólo confiere el derecho de acceso a la historia clínica al paciente, no a terceros; y el sucesivo art. 19 de ese mismo texto legal obliga a establecer "un mecanismo de custodia activa y diligente de las historias clínicas.*

*En resumen, en esta materia rige incuestionablemente la máxima confidencialidad posible, sin que haya elemento alguno en la Ley de Prevención de Riesgos Laborales o en la Ley de Autonomía del Paciente que permitan afirmar que la comunicación de datos no consentida llevada a cabo por Fremap estaba autorizada por una ley."*

Por otra parte, en el marco de la asistencia sanitaria **añade el artículo 8** que "*sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad."*

En este mismo sentido, recuerda el artículo 10.5 del Reglamento de desarrollo de la Ley Orgánica 15/1999 que "*no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud."*

Por último, **el artículo 11.2 f) de la Ley Orgánica** establece la licitud de la cesión de determinados datos relacionados con la salud si la misma es "*necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica."*

*De cuanto se lleva dicho, cabe manifestar a juicio de esta Agencia que el artículo 7.3 de la LOPD establece un régimen específico para los datos de salud, de modo que su tratamiento o comunicación podrá llevarse a cabo sin consentimiento del afectado sólo en caso de que una Ley así lo prevea, debiendo quedar esta habilitación fundada en la existencia de razones de interés general.*

De manera más rotunda, como hace el Informe de la Agencia Española de Protección de Datos 219/2008 puede decirse que "*la aplicación del artículo 7.3 de la Ley Orgánica de Protección de Datos implica, por mor del principio de especialidad, la imposible aplicación a los datos referidos en el mismo de cualquiera de las causas legitimadoras del tratamiento previstas en el artículo 11.2 de la Ley Orgánica, quedando limitados los supuestos habilitantes del tratamiento y cesión de estos datos a los establecidos en norma especial o a aquéllos en los que la norma general se refiere expresamente a tales datos."*

En consecuencia, la Ley Orgánica 15/1999 viene a establecer una lista tasada de casos en que será posible el tratamiento de los datos relacionados con la salud, quedando el mismo limitado a los supuestos en que:

- El interesado haya prestado su consentimiento expreso para ello.
- Una norma con rango de Ley así lo prevea, por razones de interés público.
- El tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, con las restricciones previstas en el artículo 7.6 de la Ley Orgánica, que deberá además ser objeto de una interpretación restrictiva, en los términos ya señalados.
- El tratamiento sea necesario para atender una urgencia vital.
- El tratamiento se lleve a cabo en el ámbito de la asistencia sanitaria respecto de los pacientes que acudan a los centros sanitarios, en los términos previstos en la legislación sectorial que resulte de aplicación.

- La comunicación de los datos sea precisa para solucionar una urgencia o para realizar los estudios epidemiológicos en los términos previstos en la legislación sectorial.

Esta normativa debe ser completada con la legislación sanitaria implicada. Hablamos de la Ley 14/1986, de 25 de abril, General de Sanidad; Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud; de la Ley 44/2003, de Ordenación de Profesiones Sanitarias; y de la Ley 8/1997, de 26 de junio, de Ordenación Sanitaria de Euskadi y hablamos, fundamentalmente, por lo que afecta a la consulta remitida igualmente a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, del Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación cínica de Euskadi y del Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

***Por tanto, a la vista de lo señalado anteriormente, debe indicarse que sólo cabría acceso a datos sanitarios sin consentimiento del afectado cuando una Ley lo prevea expresamente, debiendo quedar esta habilitación fundada en la existencia de razones de interés general.***

**II**

Una peculiaridad que tiene el tratamiento de datos de salud y de la propia historia clínica, es que la regulación de esta cuestión se trata detalladamente en la propia normativa sectorial del sector de la sanidad, y se encuentra regulado por ejemplo en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, cuyo artículo 14.1 consagra el principio de máxima integración de la misma, al disponer que "*La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro".*

En cuanto a su finalidad, el artículo 15.2 dispone que "*La historia clínica tendrá como fin principal facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud…"*.

En el mismo sentido, el Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica, en su exposición de motivos señala "…*Se trata en definitiva de una regulación de la historia clínica entendida como herramienta fundamental de los profesionales de la salud, con el objetivo de que para cada persona paciente y usuaria de los servicios sanitarios llegue a existir un soporte único con toda la información que le concierne sobre su salud, y con aplicación para todos los centros y servicios sanitarios, públicos y privados, de la Comunidad Autónoma del País Vasco".*

Indicándose en artículo 3.3 que "*Con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, la historia clínica deberá ser única, al menos en cada*

*centro sanitario o institución. Por historia clínica única se entiende la identificación de toda la documentación clínica que concierne a un o una paciente a través de un número único o excluyente para dicha persona. Este número permitirá acceder a toda su documentación clínica".*

Debe así tenerse en cuenta que el párrafo primero del artículo 56 de la Ley 16/2003, de 28 mayo, de cohesión y calidad del Sistema Nacional de Salud, dispone que *"Con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, previamente acordados con las comunidades autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione."*

En este mismo sentido, el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, recoge expresamente, sobre la base de la citada ley especial, la cesión de datos de salud en este supuesto en su artículo 10.5 disponiendo que:

> *"Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre"*
>
> *En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud."*

Por tanto, y volviendo a lo expuesto anteriormente sobre habilitación legal para la cesión de datos de salud, respecto de los centros sanitarios de la red pública, existe la habilitación legal requerida.

Igualmente y respecto de los centros sanitarios privados el artículo 44 de la Ley 14/1986, de 25 de abril, General de Sanidad señala que *"todas las estructuras y servicios públicos al servicio de la salud integrarán el Sistema Nacional de Salud",* añadiendo que "*el Sistema Nacional de Salud es el conjunto de los Servicios de Salud de la Administración del Estado y de los Servicios de Salud de las Comunidades Autónomas en los términos establecidos en la presente Ley".*

No obstante, el artículo 45 de la misma Ley 14/1986 establece que "*el Sistema Nacional de Salud integra todas las funciones y prestaciones sanitarias que, de acuerdo con lo previsto en la presente Ley, son responsabilidad de los poderes públicos para el debido cumplimiento del derecho a la protección de la salud*" y el artículo 90 habilita la celebración de conciertos con entidades sanitarias para la prestación de servicios.

Sobre estas bases, la Agencia Española de Protección de Datos ha concluido en informe de 5 de agosto de 2009 que *"En consecuencia, aún no formando parte integrante del sistema Nacional de Salud,* ***los centros concertados desarrollan acciones asistenciales directamente vinculadas con el sistema, pudiendo incluso entenderse que las mismas constituyen, en cuanto sea objeto de concierto, servicios propios del mencionado Sistema****."*

Por consiguiente, la incorporación a la historia clínica electrónica de los datos originados como consecuencia de una asistencia prestada al paciente en el marco de un concierto que mantiene con el Servicio de Salud de una Comunidad Autónoma, podría constituir una cesión de datos que resulte conforme con la Ley Orgánica 15/1999 por encontrarse amparada en el artículo 56 de la Ley 16/2003. Sí que cabe recordar en este punto que estamos hablando de centros sanitarios concertados, es decir, centros no pertenecientes al Sistema Nacional de Salud, pero que tienen relación mediante concierto con la Administración Pública correspondiente.

Por tanto, no parece que existiera vulneración de la LOPD en supuestos de acceso a la historia clínica por parte de **centros sanitarios** que integren la red del sistema nacional de salud o centros privados concertados con el Servicio de Salud de la Comunidad Autónoma como consecuencia de la atención prestada al paciente en el marco del concierto firmado.

Pero, hay que tener en cuenta, que la Ley habilitadora habla en todos los supuestos de **centros sanitarios** y no de **centros sociosanitarios,** es decir, de Residencias o Centros de Día, como es el supuesto planteado en el presente dictamen.

Cuando se habla de Residencias y Centros de Día se habla de centros sociosanitarios, se habla de centros en los que se prestan unos servicios que coordinan la asistencia curativa, social y educativa de colectivos en situación de dependencia, como la tercera edad, los enfermos crónicos y las personas con alguna discapacidad física, psíquica o sensorial y que por tanto no podemos integrarlos dentro del sistema anterior, y en los supuestos contemplados en el mismo.

Pueden existir, y es uno de los supuestos en los que habría que profundizar, centros como los expuestos que tienen exclusivamente una finalidad sanitaria, es decir, centros como los denominados “de larga estancia” en los que permanecen enfermos de edad avanzada que no pueden volver a su domicilio por ser muy dependientes que requieren cuidados paliativos, etc. En este supuesto habría que analizar su situación jurídica concreta, finalidad, etc., para determinar si se encuentran en los supuestos analizados anteriormente.

Partiendo de dicha base debemos considerar de forma general y sin perjuicio de la debida profundización que se realizará en colaboración con el Departamento, que son tres los supuestos planteados por el Departamento de Sanidad:

1. Acceso a la historia clínica de Osakidetza en Residencia y Centros día por los propios profesionales de Osakidetza que prestan asistencia sanitaria a las personas que residen o acuden a los mismos y con fines exclusivamente asistenciales.
2. Acceso a la historia clínica de Osakidetza desde Residencias y Centros de día concertados con la Administración por parte de profesionales sanitarios no dependientes de Osakidetza, y con fines exclusivamente asistenciales.
3. Acceso a la historia clínica de Osakidetza desde Residencia y Centros de Día privados no concertados por parte de profesionales sanitarios no dependientes de Osakidetza, es decir, por su propio personal sanitario y con fines exclusivamente asistenciales.

En el primer supuesto, a la vista de lo referido hasta ahora en el cuerpo del presente dictamen, una excepción a la prestación del consentimiento para el acceso a la historia clínica, la podríamos encontrar en el primero de los supuestos planteados en la consulta (como posteriormente veremos), es decir, cuando se trata de acceso a la historia clínica por los propios profesionales de Osakidetza que se desplazan a las Residencias o Centros de Día para prestar una asistencia sanitaria como red pública a las personas que residen o acuden a los centros, dado que el lugar en que se preste la asistencia sanitaria no afectaría a la habilitación legal, dado que nos encontraríamos ante la prestación de asistencia sanitaria, por un médico de la red pública sanitaria y con fines puramente asistenciales.

***Ahora bien, ante circunstancias distintas nos encontramos cuando se trata de Residencias y Centros de día en los que la asistencia sanitaria es prestada por parte de profesionales sanitarios no dependientes de Osakidetza. Teniendo en cuenta que el tratamiento y comunicación de datos de carácter personal cuyo régimen aparece recogido con carácter general en los artículos 6 y 11 de la Ley Orgánica 15/1999, se encuentra, por vía de excepción, sometido a particulares restricciones en lo que a los datos de salud respecta, por el artículo 7 de la citada Ley Orgánica, cuyo apartado 3 establece como regla general 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 y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente", siendo esta regla únicamente matizada por los artículos 7.6 y 8. Por tanto, al no existir habilitación legal expresa debemos acudir a la regla general, es decir, al consentimiento expreso del afectado como habilitación para el tratamiento de datos de salud.***

**III**

Una vez establecida la regla general del consentimiento como el principio que debe regir la implantación de este sistema, se realizarán algunas consideraciones sobre el mismo. El consentimiento se regula en el artículo 6 de la LOPD y se define en el artículo 3.h) como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen",* de lo cual se desprende la necesaria concurrencia, para que el consentimiento pueda ser considerado conforme a derecho, de los cuatro requisitos enumerados en dicho precepto.

Un adecuado análisis del concepto exige poner de manifiesto cuál es a juicio de esta Agencia la interpretación que ha de darse a estas cuatro notas características del consentimiento, siguiendo a tal efecto los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa en relación con la materia que nos ocupa.

A la luz de dichas recomendaciones, el consentimiento habrá de ser:

a) Libre, lo que supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

(Ver STS de 4-10-2002, RAJ 9797/2002, yo creo que habría que adaptar a protección de datos)

b) Específico, es decir referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999.

c) Informado, es decir que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello el artículo 5.1 de la Ley Orgánica impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen y que posteriormente será examinado.

d) Inequívoco, lo que implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

El consentimiento expreso (no necesariamente escrito, aunque hay que poder acreditar que se ha prestado), libre, inequívoco, específico e informado del propio interesado es por tanto presupuesto para el tratamiento de los datos de salud y las excepciones a dicha exigencia deben estar habilitadas en una ley dictada por razones de interés general.

Si forman parte del contenido sustancial del derecho a la protección de datos los poderes de disposición y control sobre los mismos que corresponden a sus titulares, otorgándoles dichos poderes la facultad de consentir sobre su recogida, obtención, almacenamiento y tratamiento, (de tal manera que incluso suele denominarse a tal derecho fundamental *"derecho de autodeterminación informativa"*) se comprenderá la posición angular que tal principio de consentimiento ocupa en la regulación del mismo. Este principio de consentimiento es desarrollado, además, en el RDLOPD (artículos 12 a 19), donde se regula el modo de obtención del consentimiento, el consentimiento para el tratamiento de datos de menores de edad, la forma de recabarlo y la revocación del mismo).

La legislación sectorial, en concreto la Ley 41/2002, regula el consentimiento informado (artículo 8); los límites al mismo así como el consentimiento por representación (art. 9) y las condiciones de la información y consentimiento por escrito (artículo 10).

Igualmente el Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica dedica su artículo 9.2 c) a la hoja de consentimiento informado, consentimiento que regula posteriormente en su artículo 25, al establecer:

*"Artículo 25 Consentimiento Informado*

*1.- Toda actuación en el ámbito de la salud de un o una paciente necesita el consentimiento libre, voluntario e informado de la persona afectada, del que se dejará constancia en la historia clínica.*

*2.- El o la paciente, antes de otorgar su consentimiento, tendrá derecho a la siguiente información básica:*

*a) La finalidad y los beneficios esperados con la intervención terapéutica.*

*b) Las consecuencias relevantes o de importancia asociadas a una determinada intervención.*

*c) Los riesgos relacionados con las circunstancias personales o profesionales de la persona paciente.*

*d) Los riesgos probables en condiciones normales, conforme a la experiencia y al estado de la ciencia o directamente relacionados con el tipo de intervención.*

*e) Las contraindicaciones.*

*f) Las alternativas de tratamiento existentes.*

*3.- La persona encargada de facilitar la información será el o la profesional sanitaria que prescriba la intervención y sea responsable de la asistencia, sin perjuicio de que quien practique la intervención o aplique el procedimiento pueda ayudar a aclarar los extremos que le conciernan. Se facilitará con antelación suficiente, y en todo caso, al menos 24 horas antes del procedimiento correspondiente, siempre que no se trate de actividades urgentes.*

*4.- El consentimiento se prestará de forma verbal como regla general, aunque deberá recabarse por escrito en los siguientes supuestos:*

*a) Intervenciones quirúrgicas.*

*b) Procedimientos diagnósticos y terapéuticos invasivos.*

*c) En general, en la aplicación de procedimientos que suponen riesgos e inconvenientes de notoria y previsible repercusión negativa sobre la salud de la persona paciente.*

*5.- Siempre que la persona paciente haya expresado por escrito su consentimiento informado, tendrá derecho a obtener una copia de dicho documento. El o la paciente tiene asimismo derecho a revocar libremente su consentimiento en cualquier momento sin necesidad de expresar la causa, debiendo constar dicha revocación por escrito en la historia clínica.*

*6.- El personal sanitario está exento de recoger el consentimiento informado cuando existe riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley o bien cuando existe riesgo inmediato grave para la integridad física o psíquica de la persona enferma y no sea posible conseguir su autorización, consultando en tal caso, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho.*

*7.- Se otorgará el consentimiento por representación conforme determina la Ley 41/2002 en los supuestos que contempla la misma, cuando la persona paciente a criterio médico no sea capaz de tomar decisiones por sí misma o su estado físico o psíquico no le permita hacerse cargo de su situación, cuando el paciente esté incapacitado legalmente y cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención, justificando cada criterio documentalmente."*

En este sentido, y dada la relevancia que tiene el consentimiento informado en esta cuestión y la importancia que tiene la legislación sectorial en el ámbito sanitario, habría que concretar en colaboración con la Entidad consultante, en qué supuestos cabría el consentimiento por representación, cuestión que no cabe descartar, pero que habría que modular adecuadamente, e interpretar de una forma restrictiva, y que será objeto de

análisis posterior, determinando los supuestos en que cabría dicho consentimiento por representación en aquellas situaciones en que por distintos motivos, en todo caso de naturaleza médica, el paciente no pueda emitir por sí mismo el consentimiento.

**IV**

Relacionado directa y expresamente con el consentimiento encontramos el principio de información, ya que la manifestación de los requisitos legalmente exigidos al consentimiento del paciente se realiza en la práctica a través de la información, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos específica e inequívocamente hechos constar en la mencionada información.

Este principio es de capital importancia en materia de protección de datos personales, y por ello cuenta con un exhaustivo desarrollo en el artículo 5 LOPD y en el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD.

Por tanto, para que quepa considerar que el consentimiento es informado será preciso dar cumplimiento al artículo 5.1 de la Ley Orgánica 15/1999, que establece que *"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

> *a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
>
> *b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
>
> *c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
>
> *d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
>
> *e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

Según doctrina reiterada de la Audiencia Nacional corresponde al responsable del fichero la prueba del cumplimiento del deber de informar.

Esta información en ningún caso podrá ser una información genérica, se debe informar a los pacientes de modo expreso, preciso e inequívoco de que los datos solicitados se incorporarán a la historia clínica, así como la finalidad que se dará a la información que suministre y sus derechos de acceso, rectificación, cancelación y oposición.

Por otro lado, la Recomendación sobre protección de datos médicos aconseja que la información se dé preferentemente en el momento de la recogida de datos, y que, si los datos no se obtienen directamente de la persona interesada, la información debe prestarse lo más pronto posible. Se añade que la información al titular de los datos debe ser «apropiada y adaptada a las circunstancias», y que debería informarse a cada persona individualmente.

Dada la incidencia en el tratamiento de datos de salud de estas posibles medidas, debe mencionarse igualmente el *Documento de trabajo sobre disponibilidad en red de archivos electrónicos de salud (Electronic Health Records)*, del Grupo de Trabajo internacional de protección de datos en telecomunicaciones, de abril de 2006. En concreto, sobre el derecho de información, se recomienda que el paciente sea informado de forma específica y completa de la naturaleza de los datos y de la estructura del archivo electrónico donde se contienen, por ello sería recomendable una atención especial en el derecho de información al paciente en relación con las implicaciones del tratamiento electrónico y los distintos accesos previstos.

**V**

Especial relevancia en el tratamiento de los datos sanitarios tiene igualmente el principio de calidad.

A este respecto manifestar que el artículo 3 del Decreto 38/2010, de 13 de marzo, sobre historia clínica y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica, define la historia clínica, y lo hace de una manera similar aunque no idéntica a la Ley 41/2002, disponiendo como fin principal de la historia clínica facilitar la asistencia sanitaria. La HC es desde la perspectiva de la protección de datos, un fichero (art.3b) de la LOPD), en concreto el fichero por excelencia de los datos personales de salud recabados con una finalidad sanitaria. El fin principal de la historia clínica es, precisamente, facilitar la asistencia sanitaria al paciente y por ello debe recoger la información necesaria para la prestación adecuada de la asistencia sanitaria.

En el ámbito sanitario el tratamiento de los datos se convierte en una obligación más que en una facultad, según el artículo 15.1 de la Ley 41/2002, que obliga a incorporar a la Historia Clínica la información que se considere "trascendental" para el conocimiento veraz y actualizado del estado de salud del paciente, regulando para ello su contenido mínimo (artículo 15.2). Con ello, se trataría de dar cumplimiento a un principio básico en protección de datos personales, como es el principio de calidad de los datos recogido en el artículo 4 de la LOPD.

El artículo 4.1 LOPD exige que los datos sean adecuados, pertinentes y no excesivos en relación con las finalidades para las que se hayan recabado (principio de proporcionalidad)

El artículo 4.2 LODP dispone, por su parte, que *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".*

De conformidad con este principio de finalidad recogido en el art. 4.2 de la LOPD y también en el artículo 15.1 de la Ley 41/2002**,** la recogida de datos personales únicamente puede realizarse para fines determinados, explícitos y legítimos, y el tratamiento posterior solo puede hacerse de manera compatible con esos fines**.**

A este respecto el artículo 6.1 del Decreto 38/2010, de 13 de marzo, dispone que *"la historia clínica contendrá la información suficiente para identificar a la persona paciente, apoyar el*

*diagnóstico, justificar el tratamiento, documentar la evolución y los resultados de los tratamientos y promover la continuidad de la atención entre las y los profesionales sanitarios".*

Esta previsión reglamentaria refleja la exigencia del cumplimiento de uno de los principios esenciales del derecho fundamental a la protección de datos de carácter personal, como es, el principio de calidad consagrado en el artículo 4 de la LOPD, determinándolo de forma expresa en su artículo 6.3 al señalar "*La información recogida en la historia clínica debe comprender los datos estrictamente necesarios y pertinentes, a fin de que de acuerdo al principio de calidad o proporcionalidad al que se refiere el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en ningún caso se recojan datos de las personas como pacientes que no resulten relevantes para facilitar su asistencia sanitaria ni aporten información veraz y actualizada acerca de su estado de salud".*

De conformidad con este principio de calidad no debería, en ningún caso, procederse al tratamiento de un dato del paciente si no resulta relevante para facilitar su asistencia sanitaria ni aporta información veraz y actualizada acerca de su estado de salud

Debe también tenerse presente que a tenor del artículo 4.2 de la LOPD, una vez recogidos los datos para una finalidad asistencial, únicamente puedan ser reutilizados para finalidades compatibles con aquella para la que se recogieron, en este caso, prestación de asistencia sanitaria.

**VI**

En cuanto a los diferentes supuestos planteados por el Departamento de Sanidad y en concreto respecto del acceso a la historia clínica de Osakidetza en Residencia y Centros día por los propios profesionales de Osakidetza que prestan asistencia sanitaria a las personas que residen o acuden a los mismos, parece existir habilitación legal, dado que se trata de personal de Osakidetza realizando sus labores asistenciales como médico de la red de sanidad pública en una residencia o centro de día, es decir, sería un supuesto similar a la atención domiciliaria por parte del médico de atención primaria. En este caso, lo determinante a la hora de encontrar una habilitación no sería el lugar desde donde accede el médico a la historia clínica sino su actividad como profesional sanitario que accede para la prestación de una asistencia sanitaria pública. El problema residirá fundamentalmente en el control de que se cumplan todas y cada una de las medidas de seguridad.

Así se deriva del artículo 16.1 de la Ley 41/2002, cuando señala "*… Los profesionales asistenciales del centro que realiza el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.",* disponiendo el artículo 13.2 del Decreto 38/2012 el acceso directo e inmediato a las historias clínicas de los profesionales sanitarios, sin perjuicio de que el 13.1 señale el carácter selectivo del acceso en consideración a la categoría profesional, al tipo de datos y al lugar o puesto de trabajo en relación con el proceso asistencial que se realiza.

En cuanto a los supuestos de acceso a la historia clínica de Osakidetza desde Residencias y Centros de día privados, sean estos concertados o no concertados, por parte de profesionales sanitarios no dependientes de Osakidetza y con fines exclusivamente asistenciales, debemos remitirnos al cuerpo de este informe y por tanto, al

no tratarse de centros sanitarios sino sociosanitarios y al no ser los profesionales médicos integrantes del Sistema Público de Salud, es decir, no forman parte integrante del sistema Nacional de Salud, aunque se encuentre vinculado al mismo y los pacientes sean a su vez pacientes del Servicio Vasco de Salud, se requerirá el consentimiento expreso de los afectados.

Como decíamos anteriormente, los datos sobre la salud son especialmente protegidos y esa especial protección tiene reflejo en el artículo 7.3 LOPD, que dispone que estos datos sólo podrán se recabados, tratados y cedidos cuando así lo disponga una ley por razones de interés general o el afectado lo consienta expresamente. El consentimiento expreso de sus titulares se convierte así en la regla general para el tratamiento de los datos de salud y las excepciones al consentimiento deben estar habilitadas en una ley dictada por razones de interés general.

De todos modos, debe de tenerse siempre presente que las posibles exenciones al requisito del consentimiento no significan que sea inaplicable el régimen general de protección de datos, sino al contrario, tiene especial relevancia el cumplimiento de los principios generales de la protección de datos. En concreto, la emisión del consentimiento por representación en supuestos en que médicamente no sea posible la emisión del consentimiento por la propia persona. En este caso, habrá que dejar huella fehaciente de dicho consentimiento. Los supuestos y exigencias concretas serán objeto de concreción sucesivamente y en colaboración entre la Entidad consultante y esta Agencia.

**VII**

Respecto de las medidas de seguridad, se realizará un informe complementario para establecer algunas consideraciones generales sobre esta cuestión.

**VIII**

A modo de resumen,

Sólo cabría acceso a datos sanitarios sin consentimiento del afectado cuando una Ley lo prevea expresamente, debiendo quedar esta habilitación fundada en la existencia de razones de interés general.

No existe vulneración de la LOPD en supuestos de acceso a la historia clínica por parte de centros sanitarios que integren la red del sistema nacional de salud o centros privados concertados con el Servicio de Salud de la Comunidad Autónoma como consecuencia de la atención prestada al paciente en el marco del concierto firmado.

Sin embargo, no existe previsión legal expresa que autorice el acceso a la historia clínica desde centros sociosanitarios.

Por lo tanto, será preciso obtener el consentimiento del paciente para permitir que el personal sanitario dependiente de una residencia o centro de día pueda acceder a la

historia clínica, así como acceder al mismo para proceder a su modificación, introducción de datos, etc.

Es preciso que el sistema de acceso que se establezca respete las medidas de seguridad de los datos médicos de los pacientes, en la forma que se expondrá en un informe complementario.

En el supuesto de que no sea posible obtener el consentimiento del paciente, se deberá recabar el consentimiento por representación, en los términos expuestos en este informe, y en los supuestos que se determinarán posteriormente de forma más concreta.

Vitoria-Gasteiz, 26 de diciembre de 2013

**CN13-049**

**DICTAMEN COMPLEMENTARIO SOBRE MEDIDAS DE SEGURIDAD, EN RELACIÓN A LA CONSULTA PLANTEADA POR EL DEPARTAMENTO DE SANIDAD DEL GOBIERNO VASCO RELATIVA A LOS ACCESOS A LAS HISTORIAS CLÍNICAS DE OSAKIDETZA-SERVICIO VASCO DE SALUD POR PARTE DEL PERSONAL SANITARIO DE RESIDENCIAS Y CENTROS DE DÍA.**

## ANTECEDENTES

**TERCERO:** Con fecha 28 de noviembre de 2013 se ha formulado consulta ante la Agencia Vasca de Protección de Datos en relación con el asunto arriba referenciado.

**CUARTO:** Con fecha 26 de diciembre de 2013 se dicta el dictamen CN13-049 en cuya consideración VI se manifiesta expresamente "*Respecto de las medidas de seguridad, se realizará un informe complementario para establecer algunas consideraciones generales sobre esta cuestión",* indicándose igualmente en la consideración VII "*Es preciso que el sistema de acceso que se establezca respete las medidas de seguridad de los datos médicos de los pacientes, en la forma que se expondrá en un informe complementario".*

**TERCERO:** En cumplimiento de lo anterior, se procede a la emisión del presente informe complementario sobre medidas de seguridad, en relación con el Dictamen de 26 de diciembre de 2013 relativo a la Consulta CN13-049 planteada por el Departamento de Sanidad del Gobierno Vasco.

## CONSIDERACIONES

Independientemente de la naturaleza de la relación entre las residencias y centros de día con Osakidetza que darán lugar a accesos a la historia clínica (ya sea por parte de personal sanitario de Osakidetza, de personal sanitario de residencias o centros de día concertados, o bien de personal sanitario externo actuando en residencias o centros de día no concertados), e independientemente de la naturaleza de la habilitación existente para el tratamiento en cada caso (consentimiento expreso o habilitación legal), las medidas de seguridad que habrán de ser aplicadas en cualquier caso son las que se recogen en el vigente Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (en adelante, RD-1720/2007).

El nivel de las medidas de seguridad que le corresponden al fichero de Historia Clínica Electrónica (HCE), de acuerdo con el artículo 81.3.a del RD-1720/2007, son las de ***nivel Alto*** (además de las medidas de nivel básico y medio), por ser de aplicación a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

De todo el conjunto de medidas que resultan de aplicación, nos permitimos destacar aquellas que resultan de ***especial relevancia*** para el caso que nos ocupa, dada las

concretas circunstancias en que se van a producir los accesos a la HCE desde las Residencias y Centros de día sobre los que se plantea la consulta.

Dichas medidas de seguridad son las siguientes:

### 1.- Funciones y obligaciones del personal.

Esta medida, de carácter básico, prevista en el artículo 89 del RD-1720/2007, resulta ser crucial en el caso que nos ocupa, máxime en el caso de los profesionales sanitarios de las Residencias y Centros de día no concertados en los que no existe un instrumento legal que regule su relación.

Las funciones y obligaciones, en relación con el acceso y tratamiento de los datos de la HCE, de cada uno de los perfiles de usuarios estarán claramente ***definidas y documentadas en el documento de seguridad***, al igual que las funciones de control y autorizaciones delegadas por Osakidetza. En especial, deberá recogerse entre estas obligaciones la de ***guardar el secreto profesional***, derivada del cumplimiento del artículo 10 LOPD, que obliga a todos los que intervienen en el tratamiento y que subsiste incluso después de finalizar la relación con el responsable del fichero.

Osakidetza, como responsable del fichero HCE, habrá de adoptar las medidas necesarias para que el personal ***conozca de una forma comprensible*** las normas de seguridad que afecten al desarrollo de sus funciones, así como las ***consecuencias*** en que pudiera incurrir en caso de incumplimiento. Esta difusión de las funciones y obligaciones resulta evidente en el personal propio de Osakidetza, pero debe de ser expresamente prevista respecto del personal externo, ya desempeñe su labor en Residencias y Centros de día concertados o no concertados.

En relación con esta medida, entendemos que, en el caso de las Residencias o Centros de día, concertados o no concertados, que presten asistencia sanitaria con personal externo, ***deberá existir un instrumento jurídico que regule, al menos, el acceso a la HCE por parte de dicho personal externo***, ya sea mediante un acuerdo, convenio o similar que expresamente lo regule, o bien mediante la inclusión de un clausulado específico en algún marco más amplio que ya pudiera existir.

### 2.- Identificación y autenticación de usuarios.

Deberá darse cumplimento a lo previsto en los artículos 93 y 98 del RD-1720/2007, estableciendo mecanismos que permitan la identificación de forma ***inequívoca y personalizada*** de todo usuario que deba acceder a la HCE y la verificación de que está autorizado, tal y como ya está previsto en el actual Documento de Seguridad de Osakidetza. Por lo tanto, nunca podrán existir cuentas genéricas o compartidas por varias personas.

En el caso del personal sanitario de Osakidetza que preste asistencia sanitaria a personas residentes o usuarias de los mencionados Residencias o Centros de día, con independencia del carácter concertado o no concertado de los mismos, se asume que ya figuran en el inventario de usuarios de la HCE, por lo que nada habría que añadir.

Respecto del personal sanitario no perteneciente a Osakidetza, y con independencia del carácter concertado o no concertado de las Residencias o Centros de día, deberá arbitrarse un ***procedimiento de autorización*** de estos usuarios para el acceso a las Historias Clínicas, con ***carecer previo*** a su incorporación como usuarios de la HCE, siempre teniendo en cuenta que dicho acceso podrá ser otorgado ***exclusivamente a personal sanitario***. Asimismo, existirá un procedimiento de ***actualización*** y revocación, para evitar que estos usuarios puedan ***retener privilegios*** de acceso cuando hayan cesado las circunstancias que fundamentaron la autorización. En especial, en el caso de las Residencias o Centros de día ***no concertados***, en lo que no existe otro instrumento legal que regule su relación.

## 3.- Control y registro de los accesos.

También deberá observarse lo previsto en los artículos 91, 99 y 103 del citado RD-1720/2007, a fin de controlar que los usuarios tengan ***acceso exclusivamente a aquellos recursos que precisen*** para el desarrollo de sus funciones.

Esta cuestión nos parece especialmente relevante en este ámbito, para no abrir la puerta a accesos posibles pero innecesarios a datos sanitarios que no sean imprescindibles para la finalidad que se busca.

Estos mecanismos de control habrán de establecer ***perfiles de usuario específicos para los usuarios externos*** que no pertenezcan al personal sanitario de Osakidetza. Estos perfiles específicos, diferenciados de los de su misma categoría profesional pertenecientes a Osakidetza, deberán asegurar que únicamente tienen ***acceso a los datos necesarios*** para la prestación sanitaria que deban cubrir, así como para asegurar que en ningún caso puedan ***acceder a datos de otros pacientes*** diferentes de los que se les haya autorizado en relación con su Residencia o Centro de día.

Especialmente importante resulta que el control de la concesión o revocación de estas autorizaciones de acceso estén segregadas de la Residencia o Centro de día correspondiente, reservando estas funciones de control a personal propio de Osakidetza y siempre siguiendo los criterios establecidos en el procedimiento de autorización.

Por tratarse de datos de salud, especialmente protegidos, les resulta de aplicación el artículo 103 del RD-1720/2007, exigible para los ficheros de nivel Alto de seguridad. Por lo tanto, el aplicativo de gestión deberá mantener un ***registro de los intentos de acceso***, guardándose, como mínimo, la identificación del usuario, la fecha y hora en que se realizó el intento de acceso, la identificación de la Historia que se ha pretendido acceder, el tipo de acceso o transacción y si dicho acceso ha sido autorizado o denegado, conservándose al menos durante dos años.

Este registro no podrá ser deshabilitado ni manipulado, siendo ***controlado directamente por el Responsable de Seguridad***, quien se encargará de revisarlo al menos una vez al mes, elaborando un ***informe de las incidencias*** detectadas.

## 4.- Gestión de soportes y documentos.

Aunque el contexto de los accesos sobre los cuales se plantea la consulta se centra en el acceso remoto por medios electrónicos, no es impensable que dicha información pueda ser tratada mediante su impresión e incorporación temporal a archivos no mecanizados, o almacenada temporalmente en soportes locales, como discos duros o memorias externas. Se hace hincapié en el carácter temporal de dichos tratamientos, puesto que de no tener esta componente accesoria y de limitación temporal, estaríamos hablando de la constitución de un nuevo fichero mediante la cesión de los datos de las HCS tratadas.

El tratamiento de ficheros temporales, según se establece en el artículo 87 del RD-1720/2007, deberá cumplir el mismo nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81, y será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

En el caso de que tales circunstancias pudieran llegar a darse, habrá que estar a lo previsto en los artículos 92, 97 y 101 del RD-1720/2007, respecto de la gestión de soportes. En particular, habrá de tenerse en cuenta que cuando la información sea transmitida por redes públicas o redes inalámbricas o sea almacenada en dispositivos portátiles, deberán contener la información en forma cifrada y que siempre que estos últimos vayan a desecharse deberá procederse a su destrucción o borrado, impidiendo el acceso a la información contenida en el mismo o su recuperación posterior.

Asimismo, respecto de los tratamientos no automatizados, deberán observarse las precauciones contenidas en los artículos 106 a 114 del RD-1720/2007, limitándose el acceso a tales documentos exclusivamente al personal autorizado, cuidando que sean almacenados en armarios o archivadores con sistema de apertura mediante llave o similar, y cuidando que las copias o impresiones se efectúan siempre de forma controlada, adoptándose respecto de la destrucción de las mismas las cautelas ya apuntadas que eviten su recuperación posterior.

## 5.- Organización de la seguridad.

Todas las anteriores medidas deberán estar documentadas tal como se exige en el artículo 88 del RD-1720/2007, manteniéndose el Documento de Seguridad que allí se describe actualizado en todo momento y recogiendo todos los aspectos que en él se detallan.

Las medidas de seguridad, en concreto todas las relacionadas con los accesos a la HCE por personal externo, deben someterse a auditoría al menos cada dos años, de acuerdo con lo previsto en los artículos 96 y 110 del RD-1720/2007, debiendo dichas auditorías dictaminar sobre la adecuación de las medidas y controles, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Vitoria-Gasteiz, 30 de diciembre de 2013