Grupo de Trabajo sobre protección de datos del artículo 29

00323/07/ES
WP 131

Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)

Adoptado el 15 de febrero de 2007

SÍNTESIS

En este documento de trabajo sobre **el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME),** el Grupo de Trabajo del artículo 29 proporciona una orientación sobre la interpretación del marco jurídico aplicable en materia de protección de datos para los sistemas de HME, y explica algunos de los principios generales. El documento de trabajo también proporciona indicaciones sobre los requisitos de protección de datos que deben cumplir los sistemas de HME, así como sobre las garantías aplicables.

El Grupo de Trabajo del artículo 29 examina en primer lugar **el marco jurídico general de la protección de datos** para los sistemas de HME. El Grupo de Trabajo del artículo 29 recuerda la prohibición general de tratamiento de datos personales relativos a la salud, prevista en el artículo 8, apartado 1, de la Directiva 95/46/CE sobre protección de datos, y posteriormente discute la posible aplicación de las excepciones previstas en el artículo 8, apartados 2, 3 y 4 de la Directiva en el contexto de los sistemas de HME, subrayando la necesidad de interpretar tales excepciones de forma restrictiva.

El Grupo de Trabajo del artículo 29 también reflexiona sobre **un marco jurídico adecuado para los sistemas de HME,** y proporciona **recomendaciones sobre once cuestiones** para las que parece especialmente necesario establecer garantías especiales en los sistemas de HME a fin de garantizar los derechos de protección de datos de los pacientes y de las personas. Estas cuestiones son las siguientes:

1. Respeto de la autodeterminación
2. Identificación y autenticación de los pacientes y los profesionales de la salud
3. Autorización para acceder a los HME a efectos de lectura y de escritura
4. Uso de los HME para otras finalidades
5. Estructura organizativa de un sistema de HME
6. Categorías de datos almacenados en los HME y modos de presentación
7. Transferencia internacional de historiales médicos
8. Seguridad de los datos
9. Transparencia
10. Cuestiones relacionadas con la responsabilidad
11. Mecanismos de control para el tratamiento de los datos contenidos en los HME

El Grupo de Trabajo del artículo 29 invita a la profesión médica, a todos los profesionales de la salud, a todas las personas e instituciones implicadas, así como al público en general, a que presenten comentarios sobre este documento de trabajo.

ÍNDICE

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES,

Vista 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[1], y, en particular, su artículo 29 y su artículo 30, apartado 1, letra b),

Visto el reglamento interno del Grupo[2] y, en particular, sus artículos 12 y 14,

HA ADOPTADO EL SIGUIENTE DOCUMENTO DE TRABAJO:

I. Introducción

El objetivo del presente documento de trabajo del Grupo de Trabajo del artículo 29 es proporcionar una orientación sobre la interpretación del marco jurídico aplicable en materia de protección de datos a los sistemas de historiales médicos electrónicos (HME), y establecer algunos principios generales. También aspira a definir los requisitos de protección de datos para el establecimiento de un sistema de HME a escala nacional, así como las garantías aplicables.

Los costes de los sistemas públicos de salud están aumentando drásticamente, y los gobiernos necesitan nuevas estrategias para abordar este problema. Una de las respuestas que suele darse es el "historial médico electrónico (HME)". Entre los términos empleados en este ámbito figuran el de "historial de salud electrónico", "historial electrónico del paciente", "historial informatizado del paciente", etc., que pueden emplearse indistintamente.

A efectos del presente documento de trabajo, por "historial médico electrónico" (en adelante: HME) se entiende lo siguiente:

> *"un historial médico completo o una documentación similar del estado de salud física y mental pasado y presente de un individuo, en formato electrónico, que permita acceder fácilmente a estos datos a efectos de tratamientos médicos y otros fines estrechamente relacionados*[3]*."*

Tradicionalmente, la documentación sobre tratamientos médicos estaba en poder de los distintos profesionales de la salud, pero no figuraba en un único historial. Por su parte, el concepto de "HME" aspira a recoger la documentación existente sobre los tratamientos médicos de un individuo, a partir de diversas fuentes y en distintos momentos. Por tanto, proporcionaría información sobre el estado de salud pasado y presente de un individuo de la forma más amplia posible, y para un período de tiempo considerable, quizás incluso toda la vida ("*de la cuna al sepulcro").* Una vez compilados, los datos del HME estarían disponibles

[1] Directiva CE/95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que con respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281, 23.11.1995, p. 31 (en lo sucesivo: "la Directiva"), disponible en: http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

[2] Adoptado por el Grupo en su tercera reunión celebrada el 11.9.1996.

[3] "Tratamientos médicos y otros fines estrechamente relacionados" hace referencia a los fines mencionados en el apartado 3 del artículo 8 de la Directiva.

en formato electrónico para todos los profesionales sanitarios autorizados y otras instituciones autorizadas dondequiera y siempre que esta información fuere necesaria.

El HME se presenta como un medio apropiado para:

- lograr una mejor calidad del tratamiento gracias a una mejor información sobre el paciente;
- mejorar la relación coste-eficacia de los tratamientos médicos y prevenir así el crecimiento rápido de los déficit del presupuesto de la salud;
- suministrar los datos necesarios para el control de calidad, las estadísticas y la planificación del sector público de salud, lo que deberá tener también un efecto positivo en los presupuestos públicos de salud.

Las respuestas a un cuestionario distribuido en 2005 entre las autoridades nacionales de control de protección de los datos pusieron de manifiesto que los sistemas de HME nacionales son una cuestión pertinente y urgente en la mayoría de los Estados miembros. Sin embargo, el grado de ejecución de tales proyectos difiere ampliamente: mientras que la mayoría de los Estados miembros están discutiendo sobre los HME, otros ya han aplicado al menos parcialmente los sistemas de HME.

Debido al hecho de que la atención sanitaria se presta cada vez más de forma transfronteriza, la Comisión Europea ha subrayado, en su Comunicación "*La salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica*"[4], la importancia de los servicios sanitarios electrónicos y de la interoperabilidad de los historiales médicos electrónicos. Además, la Comunidad Europea está financiando proyectos pertinentes, por ejemplo sobre los historiales electrónicos de los pacientes o sobre los identificadores de los pacientes (por ejemplo, la tarjeta sanitaria europea). Al aplicar estos programas, la Comisión Europea está obligada, junto con los Estados miembros, a garantizar el cumplimiento de todas las disposiciones legales pertinentes relativas a la protección de los datos personales y, en su caso, a la introducción de mecanismos dirigidos a garantizar la confidencialidad y la seguridad de tales datos[5].

Los sistemas de HME tienen el potencial para lograr una mayor calidad y seguridad en la información médica que las formas tradicionales de documentación médica. Sin embargo, desde el punto de vista de la protección de datos, hay que subrayar el hecho de que los sistemas de HME, además, tienen potencial no sólo para tratar más datos personales (por ejemplo, en nuevos contextos, o por agregación), sino también para hacer que los datos de los pacientes sean más fácilmente accesibles para un numero mayor de destinatarios.

Cabe también señalar que la información sanitaria electrónica contenida en un sistema de HME, aparte de ser accesible para los profesionales sanitarios, podría atraer en general el interés de terceros, tales como compañías de seguros y servicios de seguridad del Estado. Desde el punto de vista de la protección de datos personales, al compilar la información médica existente sobre un individuo, procedente de diversas fuentes, con el fin de permitir un acceso más fácil y más amplio a esta información sensible, los sistemas de HME introducen una nueva situación de riesgo, cambiando toda la escala de posible uso ilícito de la información médica sobre los individuos. Si bien esta nueva situación de riesgo sólo se dará en la mayoría de los proyectos cuando se apliquen plenamente, es sin embargo necesario ser

[4] COM(2004) 356 final.

[5] Véase, por ejemplo el artículo 5, apartado 5, de la Decisión 1786/2002/CE.

consciente ahora de estos peligros, cuando la mayoría de los modelos existentes sólo prevén una aplicación limitada o parcial (por ejemplo, relativa únicamente a un conjunto básico de datos médicos o a los hospitales de una región determinada), puesto que es sólo cuestión de tiempo antes de que lleguen a ser generalmente aplicables.

II. El marco de protección de datos aplicable a los historiales médicos electrónicos

Todo tratamiento de datos personales en los sistemas de HME tiene que cumplir plenamente con las normas de protección de datos personales. El Grupo de Trabajo desearía subrayar que el marco aplicable al uso de HME figura en el considerando 2 de la Directiva, que establece lo siguiente: "*Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales de las personas físicas y, en particular, la intimidad, y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos*".

El derecho fundamental a la protección de datos personales se basa esencialmente en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (ECHR) y en el artículo 8 de la Carta de los Derechos Fundamentales de la UE[6]. Normas más específicas figuran en la Directiva 95/46/CE sobre protección de datos y en la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas[7], así como en las leyes nacionales de los Estados miembros que aplican estas Directivas.

Todo tratamiento de datos personales en los HME debe cumplir asimismo con las normas establecidas en el Convenio del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (ETS nº 108), y en el Protocolo adicional al Convenio 108, relativo a las autoridades de control y los tránsitos transfronterizos de datos. (ETS nº 181).

En el contexto de los HME, el Grupo de Trabajo desearía subrayar de forma específica la importancia de la Recomendación nº R (97) 5 del Consejo de Europa sobre la protección de datos médicos (13 de febrero de 1997). También se hace referencia a las recomendaciones presentadas en el "documento de trabajo sobre la disponibilidad en línea de los historiales médicos electrónicos" por el Grupo de trabajo internacional sobre protección de datos en las telecomunicaciones[8].

---

[6] El derecho a la protección de los datos personales no es absoluto, y puede restringirse si intereses públicos específicos así lo requieren. Sin embargo, no podrá haber ingerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta ingerencia esté prevista por ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás, y no sea desproporcionada con respecto al objetivo que se persiga (apartado 2 del artículo 8 ECHR).

[7] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201 de 31.7.2002, p. 37).

[8] Adoptado en su 39ª reunión en Washington D.C., 6-7 de abril de 2006 (http://www.berlin-privacy-group.org).

1. Principios generales

Los responsables del tratamiento de los datos que recogen datos en el contexto de las aplicaciones HME deben por tanto cumplir todos los principios generales de protección de datos, incluidos los siguientes:

- Principio de limitación de uso (principio de propósito): este principio, incluido parcialmente en el artículo 6, apartado 1, letra b), de la Directiva, prohíbe entre otros un tratamiento posterior que sea incompatible con la finalidad de su recogida.
- Principio de calidad de los datos: este principio, en la Directiva, exige que los datos personales sean pertinentes y no excesivos para los fines para los que se recogen. Así pues, no debe recogerse ningún dato irrelevante, y si se recoge, debe desecharse (artículo 6(1) (c)). También exige que los datos sean exactos y estén actualizados.
- Principio de retención: este principio exige que los datos personales se conserven como máximo durante el tiempo necesario para el propósito para el que se recabaron o se trataron.
- Requisitos en materia de información: de conformidad con el artículo 10 de la Directiva, los responsables del tratamiento de datos en sistemas de HME deberán comunicar al interesado determinada información, tal como la identidad del responsable del tratamiento, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los datos y la existencia de derechos de acceso.
- Derecho de acceso del interesado: el artículo 12 de la Directiva establece que los interesados podrán verificar la exactitud de los datos y asegurarse de que éstos estén actualizados. Estos derechos se aplican plenamente a la recogida de datos personales en los sistemas de HME.
- Obligaciones relacionadas con la seguridad: el artículo 17 de la Directiva establece la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción accidental o ilícita o la difusión no autorizada. Las medidas pueden ser organizativas o técnicas.

2. Protección especial para datos personales sensibles

Sin embargo, cuando el tratamiento de estos datos personales se refiere a la salud de una persona, es particularmente sensible y por tanto requiere una protección especial.

El artículo 2, letra a), de la Directiva 95/46/CE define los datos personales del siguiente modo:

"«datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

El artículo 8, apartado 1, de la Directiva define las categorías especiales de datos del siguiente modo:

"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 indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud en el sentido del artículo 8, apartado 1, de la Directiva 95/46[9]. Esta definición también se aplica a los datos personales cuando tienen una relación clara y estrecha con la descripción del estado de salud de una persona: los datos sobre el consumo de medicamentos, alcohol o drogas, así como los datos genéticos, son sin duda "datos personales sobre la salud", especialmente si están incluidos en un expediente médico. También habrá que considerar sensibles otros datos - por ejemplo, los datos administrativos (número de seguridad social, fecha de ingreso en un hospital, etc.) - contenidos en la documentación médica relativa al tratamiento de un paciente: si no fueran pertinentes en el contexto del tratamiento del paciente, no se habrían incluido, ni deberían haberse incluido, en un expediente médico.

Por consiguiente, los miembros del Grupo de Trabajo opinan que todos los datos contenidos en documentos médicos, en historiales médicos electrónicos y en sistemas de HME son "datos personales sensibles". Por tanto, no sólo están sujetos a todas las normas generales sobre protección de datos personales de la Directiva, sino también a las normas sobre protección de datos especiales que rigen el tratamiento de la información sensible, contenidas en el artículo 8 de la Directiva.

3. Prohibición general del tratamiento de datos personales relativos a la salud - con excepciones

El artículo 8, apartado 1, de la Directiva 95/46/CE sobre protección de datos prohíbe el tratamiento de los datos personales relativos a la salud en general. Lo mismo hace el artículo 6 del Convenio n° 108 del Consejo de Europa.

Esta protección especial contenida en el artículo 8, apartado 1, complementa las otras disposiciones de la Directiva, en especial el artículo 6 sobre los principios relativos a la calidad de los datos, y el artículo 7 sobre los principios relativos a la legitimación del tratamiento de datos.

Sin embargo, teniendo en cuenta la importancia de utilizar la información sobre un paciente para tratarlo médicamente como corresponde, hay excepciones a la prohibición general de tratamiento de los datos médicos.

La Directiva sobre protección de datos establece unas **excepciones obligatorias** en el artículo 8, apartados 2 y 3, y **una excepción opcional** en el apartado 4.

Todas estas excepciones son **limitadas**, **exhaustivas** y deben **interpretarse de forma restrictiva**.

4. Artículo 8, apartado 2, letra a): "consentimiento explícito"

Según el artículo 8, apartado 2, letra a), de la Directiva:

> *"Lo dispuesto en el apartado 1 no se aplicará cuando: el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado,"*

[9] Tribunal de Justicia de las Comunidades Europeas, sentencia de 6 de noviembre de 2003, asunto C-101/01 - Bodil Lindqvist.

a) Por tanto, una justificación para el tratamiento de datos sensibles puede ser el **consentimiento** del interesado[10]. Como ya se indicó en los documentos WP 12[11] y WP 114[12] previos del Grupo de Trabajo, un elemento importante es que para ser válido, el consentimiento - independientemente de las circunstancias en que se exprese - debe ser una *"manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan"*, según lo definido en la letra h) del artículo 2 de la Directiva.

aa) El consentimiento debe darse libremente: el consentimiento "libre" supone una decisión voluntaria, de un individuo en posesión de todas sus facultades, tomada sin ningún tipo de coacción, ya sea social, financiera, psicológica u otra. El consentimiento dado bajo amenaza de no tratamiento o de tratamiento de menor calidad en una circunstancia médica no puede considerarse "libre". No se puede considerar válido el consentimiento dado por un interesado que no haya tenido la oportunidad de hacer una verdadera elección o que se haya encontrado frente a un hecho consumado.

El Grupo de Trabajo del artículo 29 considera que, cuando como consecuencia necesaria e inevitable de la circunstancia médica un profesional de la salud tenga que tratar datos personales en un sistema de HME, es equívoco que este profesional intente legitimar este tratamiento a través del consentimiento. El recurso al consentimiento debe limitarse a los casos en que el interesado tenga una auténtica libertad de elección y por tanto sea posteriormente capaz de retirar el consentimiento sin sufrir perjuicio alguno[13].

bb) El consentimiento debe ser específico: el consentimiento "específico" debe referirse a una situación bien definida y concreta en que esté previsto el tratamiento de datos médicos. Por tanto, un "acuerdo general" del interesado, por ejemplo para la recogida de sus datos médicos para un HME y las posteriores transferencias de estos datos médicos del pasado y del futuro a profesionales sanitarios implicados en el tratamiento no constituiría consentimiento con arreglo a lo dispuesto en la letra h) del artículo 2 de la Directiva.

cc) El consentimiento debe ser con conocimiento de causa: un consentimiento "informado" por parte del interesado supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción. El individuo afectado debe contar con información exacta y completa, dada de forma clara y comprensible, sobre todas las cuestiones pertinentes, en especial las especificadas en los artículos 10 y 11 de la Directiva, tal como la naturaleza de los datos tratados, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los mismos

[10] La aceptación de seguir un tratamiento médico determinado no supone automáticamente el "consentimiento", en el sentido de la letra h) del artículo 2, al tratamiento (especialmente la comunicación o la transferencia) de los datos personales recogidos durante dicho tratamiento médico.

[11] Grupo de Trabajo del artículo 29 "Documento de trabajo: Transferencias de datos personales a los terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos" (WP 12, 24 de julio de 1998).

[12] Grupo de Trabajo del artículo 29 "Documento de trabajo sobre una interpretación común del apartado 1 del artículo 26 de la Directiva 95/46/CE de 24 de octubre de 1995" (WP 114, 25 de noviembre de 2005).

[13] Véase también el "Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto del empleo" del Grupo de Trabajo del artículo 29 (WP 84, sección 10).

y los derechos del interesado. Esto incluye también el conocimiento de las consecuencias de no consentir el tratamiento de los datos en cuestión.

b) En contraste con lo previsto en el artículo 7 de la Directiva, el consentimiento en el caso de los datos personales sensibles y por tanto de un HME debe ser **explícito**. Las soluciones consistentes en entender que existe una autorización tácita si no se manifiesta explícitamente lo contrario, no cumplirán el requisito de ser "explícitas". De conformidad con la definición general de que el consentimiento presupone una declaración de intenciones, la explicitud debe referirse, en especial, **al carácter sensible de los datos**. El interesado debe ser consciente de que está renunciando a una protección especial. No obstante, no se requiere un consentimiento escrito.

c) El Grupo de Trabajo del artículo 29 ha observado que a veces resulta complicado obtener el consentimiento debido a problemas prácticos, en especial cuando no hay un contacto directo entre el responsable de los datos y el interesado. Cualesquiera que sean las dificultades, **el responsable del tratamiento** debe poder probar en todos los casos, en primer lugar, que ha obtenido el consentimiento explícito de cada interesado y, en segundo lugar, que este consentimiento explícito se dio basándose en información suficientemente exacta.

d) De nuevo en contraste con el artículo 7, el artículo 8, apartado 2, letra a) reconoce que puede haber casos de tratamiento de datos sensibles en que **ni siquiera el consentimiento explícito** del interesado pueda levantar la prohibición de tratamiento: los Estados miembros tienen libertad para regular tales casos detalladamente.

5. Artículo 8, apartado 2, letra c): "interés vital del interesado"

El tratamiento de datos personales sensibles puede justificarse si es necesario proteger los intereses vitales del interesado o de otra persona, cuando el interesado sea física o jurídicamente incapaz de dar su consentimiento.

El tratamiento debe referirse a intereses individuales esenciales del interesado o de otra persona, y debe - en el contexto médico - ser necesario para un tratamiento médico dirigido a salvar la vida en una circunstancia en que el interesado no esté en condiciones de expresar sus intenciones. Por consiguiente, esta excepción sólo puede aplicarse a un pequeño número de casos de tratamiento y no puede utilizarse en absoluto para justificar el tratamiento de datos médicos personales con fines distintos del tratamiento del interesado, como por ejemplo realizar investigaciones médicas generales que sólo darán resultados en el futuro[14].

Por ejemplo: supongamos que un interesado ha perdido la consciencia después de un accidente y no puede dar su consentimiento para la revelación necesaria de alergias conocidas. En el contexto de los sistemas de HME, esta disposición permitiría el acceso a la información almacenada en el HME a un profesional de la salud con el fin de extraer datos sobre alergias conocidas del interesado, que pueden resultar decisivos para el tratamiento elegido.

[14] Para una interpretación de la disposición similar contenida en el artículo 26, apartado 1, letra e) por lo que se refiere a transferencias de datos fuera de la UE, véase el "Documento de trabajo sobre una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995", WP 114, del Grupo de Trabajo del artículo 29 (25 de noviembre de 2005).

6. Artículo 8, apartado 3: “tratamiento de datos (médicos) realizado por un profesional de la salud”

El artículo 8, apartado 3, permite el tratamiento de datos personales sensibles siempre que se cumplan tres condiciones acumulativas: el tratamiento de datos personales sensibles debe ser “*necesario”*, debe realizarse *“para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios”,* y el tratamiento de los datos personales en cuestión deberá ser *“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”*.

a) 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 quedan 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 del 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.

b) Además, el tratamiento de datos personales contemplado en el apartado 3 del artículo 8 deberá ser **“necesario”** para los fines específicos mencionados en la letra a). El Grupo de Trabajo subraya que esto significa, en un contexto de HME, que habría que justificar plenamente cualquier inclusión de datos personales en un HME; la mera “utilidad” de tener tales datos personales en un HME no sería suficiente.

c) La tercera condición prevista en el apartado 3 del artículo 8 es que el tratamiento de datos personales sensibles debe ser realizado por un profesional sanitario o por otra persona sujeta asimismo al **secreto (médico) profesional o a una obligación equivalente de secreto.**

> El requisito ético de confidencialidad de la profesión médica se estableció por primera vez en el “juramento hipocrático”[15], y fue confirmado posteriormente por la Declaración de Ginebra de la Asociación Médica Mundial (1948). Protege la información obtenida por los profesionales sanitarios en el curso del tratamiento de un paciente. El uso de esta información se permite sólo dentro de los límites del contrato de tratamiento. Esta relación de confidencialidad excluye a cualquier tercero, incluso a otros profesionales sanitarios, a menos que el paciente haya autorizado la transmisión de sus datos o esto se prevea especialmente por ley.

El Grupo de Trabajo señala que la obligación especial de secreto profesional debe ser establecida bien por el Derecho nacional de los Estados miembros, o por los organismos profesionales nacionales competentes con poder para adoptar normas vinculantes sobre la profesión. Estas normas nacionales de secreto profesional deben también prever sanciones efectivas en caso de incumplimiento.

---

[15] *“Guardaré silencio sobre todo aquello que en mi profesión, o fuera de ella, oiga o vea en la vida de los hombres que no deba ser público, manteniendo estas cosas de manera que no se pueda hablar de ellas.”* (Fuente: http://es.wikipedia.org/wiki/Juramento_hipocrático).

Según la Directiva, en caso de que surja la necesidad de que personal no médico trate estos datos personales sensibles, este personal también deberá estar sujeto a normas vinculantes que garanticen al menos un nivel equivalente de confidencialidad y protección. En especial, estas normas deberán contener la obligación de que los datos se utilicen solamente para los fines mencionados en el artículo 8, apartado 3.

Los profesionales sanitarios con responsabilidad directa en el tratamiento de pacientes tienen generalmente la obligación legal de conservar la documentación sobre su tratamiento médico (acciones, prescripciones, etc.) en los historiales de los pacientes. De conformidad con las numerosas disposiciones legales existentes sobre la obligación de secreto profesional de los profesionales sanitarios, la conservación y uso de los historiales de los pacientes están tradicionalmente limitados a la relación bilateral directa entre un paciente y el profesional sanitario o la institución sanitaria consultados por el paciente.

d) Puesto que el artículo 8, apartado 3, de la Directiva constituye una excepción a la prohibición general de tratar datos sensibles, esta excepción deberá interpretarse de forma restrictiva.

e) En caso de que se planteara la cuestión de si el apartado 3 del artículo 8 de la Directiva puede servir como *única* base jurídica para el tratamiento de datos personales en un sistema de HME, el Grupo de Trabajo del artículo 29 opina que el apartado 3 del artículo 8 sólo se refiere al tratamiento de datos médicos para los estrictos fines médicos y sanitarios mencionados en el mismo, y estrictamente con las condiciones de que el tratamiento "sea necesario" y sea realizado por un profesional sanitario o por otra persona sujeta asimismo a una obligación equivalente de secreto. En los casos en que el tratamiento de datos personales contenidos en un HME vaya más allá de estos fines o no cumpla dichas condiciones, el apartado 3 del artículo 8 no podrá servir como única base jurídica para el tratamiento de esos datos personales.

Sin embargo, incluso si se cumplieran todos estos requisitos previos, el Grupo de Trabajo del artículo 29 señala que los sistemas de HME crean una nueva situación de riesgo, que exige garantías nuevas adicionales en contrapartida: los sistemas de HME proporcionan acceso directo a una compilación de la documentación existente sobre el tratamiento médico de una persona específica, procedente de diversas fuentes (por ejemplo, hospitales o profesionales sanitarios) y a lo largo de una vida. Por tanto, estos sistemas de HME superan los límites tradicionales de la relación directa de cada paciente con un profesional o una institución sanitaria. La conservación de información médica en un HME va más allá de los métodos tradicionales de conservación y uso de la documentación médica sobre los pacientes. Por lo que respecta al aspecto técnico, la multiplicidad de puntos de acceso en una red abierta como Internet aumenta la posible interceptación de datos de los pacientes. El mantenimiento de la norma jurídica de confidencialidad que resulta adecuada en un medio tradicional de documentos en papel puede ser insuficiente para proteger la intimidad de un paciente una vez que los historiales médicos electrónicos se ponen en línea. Los sistemas de HME plenamente desarrollados tienden así a abrir y a facilitar el acceso a la información médica y a los datos personales sensibles. Los sistemas de HME plantean considerables retos a la hora de garantizar que sólo los profesionales sanitarios habilitados accedan a la información con fines legítimos relacionados con el tratamiento del interesado. Estos sistemas hacen que el tratamiento de datos personales sensibles sea más complejo, con consecuencias directas para los derechos de los individuos. Por consiguiente, un sistema de HME debe considerarse una nueva situación de riesgo para la protección de los datos personales sensibles.

La garantía principal y tradicional del artículo 8, apartado 3 - aparte de la limitación del propósito y del requisito estricto de necesidad - es la obligación de confidencialidad de los profesionales médicos por lo que respecta a los datos médicos sobre sus pacientes. Esto puede

ya no ser plenamente aplicable en un medio de HME, pues uno de los fines del HME es proporcionar acceso a la documentación médica con fines de tratamiento a profesionales que no hayan tomado parte en los tratamientos anteriores documentados en un historial médico.

Por tanto, el Grupo de Trabajo del artículo 29 no está convencido de que, incluso si se utilizara el apartado 3 del artículo 8 como justificación para el tratamiento de datos, el basarse solamente en la obligación de secreto profesional proporcione protección suficiente en el caso de los HME. Una nueva situación de riesgo exige garantías adicionales y posiblemente nuevas, más allá de las requeridas por el apartado 3 del artículo 8, para prever una protección adecuada de los datos personales en un contexto de HME.

7. Artículo 8, apartado 4: excepciones por motivos de interés público importantes

Varias disposiciones de la Directiva contienen un considerable grado de flexibilidad, con el fin de alcanzar el equilibrio adecuado entre, por una parte, la protección de los derechos del interesado, y por otra parte, los intereses legítimos de los responsables del tratamiento de los datos, de terceras partes y el interés público que pueda existir.

El apartado 4 del artículo 8 de la Directiva permite a los Estados miembros establecer otras excepciones a la prohibición del tratamiento de categorías de datos sensibles:

> *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 nacional, bien por decisión de la autoridad de control.*
>
> El considerando 34 reza como sigue:
>
> *Considerando que también 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 de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro 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;*

a) Por consiguiente, en caso de que un Estado miembro se proponga hacer uso de esta posibilidad, la excepción debe figurar en una disposición legal o en una decisión de la autoridad supervisora (**base jurídica especial**).

b) Tal tratamiento de datos personales sensibles debe estar justificado por motivos **de interés público importantes**. El considerando 34 de la Directiva proporciona ejemplos de ámbitos que son particularmente propensos a incluir casos de “interés público importante”. Entre éstos figuran los ámbitos de la salud pública y la protección social, particularemente en lo relativo a la garantía de la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad.

En cada caso, el conjunto del tratamiento 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"*.

c) Los Estados miembros están obligados a proporcionar **garantías específicas y adecuadas** a fin de proteger los derechos fundamentales y el derecho a la vida privada de las personas en ese contexto.

d) Todo uso del apartado 4 del artículo 8 por parte de un Estado miembro deberá **notificarse a la Comisión** de conformidad con el apartado 6 del artículo 8 de la Directiva.

En el contexto de los HME, el Grupo de Trabajo del artículo 29 observa que los argumentos a favor de la introducción de los sistemas de HME (véase el apartado I *supra*) pueden determinar el "interés público importante". En algunos Estados miembros, el derecho a la protección de la salud está consagrado en la Constitución. Esto subraya la importancia que se atribuye a todos los medios adecuados de lograr una "protección de la salud". Un sistema de HME en tales medios jurídicos se basaría ciertamente en el "interés público importante", pues se trata de un instrumento fundamentalmente destinado a garantizar una asistencia médica adecuada a los pacientes.

El apartado 4 del artículo 8 de la Directiva puede, por tanto, servir de base jurídica para los sistemas de HME, siempre que se cumplan todas las condiciones mencionadas en el mismo. En particular, deberán preverse garantías adecuadas para la protección de los datos personales en un sistema de HME.

En la siguiente sección, el Grupo de Trabajo presenta una reflexión sobre estas posibles garantías y sobre el marco jurídico adecuado para los sistemas de HME.

III. Reflexión sobre un marco jurídico adecuado para los sistemas de HME

El Grupo de Trabajo del artículo 29 proporciona información sobre aquellos temas para los que resulta especialmente necesario establecer garantías especiales[16] en los sistemas de HME a fin de garantizar los derechos de protección de datos de los pacientes. Habida cuenta del impacto de los sistemas de HME y de la necesidad especial de garantizar su transparencia, las garantías deberán establecerse preferiblemente en un marco jurídico amplio específico.

[16] Los requisitos generales previstos en la Directiva 95/46/CE para el tratamiento lícito de los datos personales no se repiten en esta parte del documento, dado que se aplican de todos modos. El presente documento sólo desarrolla los requisitos adicionales específicos para tratar datos médicos en los sistemas de HME, que parecen necesarios para contrarrestar la situación especial de riesgo a la intimidad causada por los sistemas de HME.

1. Respeto de la autodeterminación

Incluso si un sistema de HME no se basa enteramente en el consentimiento como base jurídica (artículo 8 (2)), la autodeterminación del paciente por lo que respecta a cuándo y cómo se utilizan sus datos debería constituir una garantía importante[17].

a) El "acuerdo" del paciente en el contexto de las garantías adecuadas es diferente del "consentimiento" de conformidad con el apartado 2 del artículo 8 de la Directiva, y por tanto no necesita cumplir todos los requisitos del apartado 2 del artículo 8: por ejemplo, mientras que **el consentimiento como base jurídica** para el tratamiento de datos sobre la salud tendría que ser siempre explícito de acuerdo con el apartado 2 del artículo 8, **el acuerdo como garantía** no debe darse necesariamente en forma de consentimiento previo; la posibilidad de expresar la autodeterminación podría, dependiendo de la situación, ofrecerse también en forma de derecho de denegación.

b) A la vista del potencial de perjuicio variable que revisten los distintos tipos de información sobre la salud, deberían establecerse categorías de utilizacion con **distintos grados de posibilidad de ejercer la autodeterminación**:

Las disposiciones jurídicas que introducen un sistema de HME debe establecer por norma general el consentimiento previo del paciente para la introducción de datos en un HME o el acceso a tales datos (especialmente por lo que respecta al tratamiento de datos susceptibles de utilizarse de forma perjudicial, como por ejemplo datos psiquiátricos, datos sobre abortos, etc.[18]), y prever la posibilidad de denegación por lo que respecta a datos menos íntimos[19]. Esto podría garantizar el nivel de protección necesaria por una parte, y la viabilidad y flexibilidad necesarias, por otra.

c) Siempre debería ser **posible**, en principio, **que un paciente impida la comunicación** de sus datos médicos, documentados por un profesional de la salud durante el tratamiento, a otros profesionales de la salud, si así lo decide.

También debería estudiarse la cuestión de cómo tratar la supresión del acceso a la información contenida en un HME: ¿debe enmascararse tal supresión para que sea indetectable, o en determinados casos debe darse un mensaje en el sentido de que existe información adicional pero que sólo está disponible en condiciones muy concretas?

d) En el supuesto de que nadie pueda verse obligado a participar en un sistema de HME, es necesario que las disposiciones jurídicas que establezcan un sistema de HME prevean la **posibilidad de retirada total de un sistema de HME**. Deben preverse normas que determinen si esta retirada supone la obligación de suprimir completamente los datos del sistema de HME o simplemente de impedir el acceso a los mismos; también puede darse la opción a los interesados.

---

[17] En algunos países existe no sólo un derecho fundamental a la protección de datos, sino también un derecho constitucional a una protección óptima de la salud: como consecuencia de esta obligación de proporcionar un tratamiento óptimo, algunos Estados miembros han otorgado a los profesionales de la salud un acceso obligatorio a los datos disponibles a través del sistema de HME. Esto parece aceptable siempre que se alcance el equilibrio necesario mediante otras garantías, tales como normativas detalladas sobre las circunstancias del acceso legítimo, graves consecuencias en caso de uso abusivo de los derechos de acceso, etc.

[18] Podrían utilizarse elementos especiales como "sobres sellados", que no pueden abrirse sin la cooperación del interesado.

[19] Para que las soluciones de denegación constituyeran una "garantía adecuada" eficaz sería necesario que el paciente reciba información adecuada.

2. Identificación y autenticación de los pacientes y de los profesionales de la salud

a) Una **identificación fiable**[20] **de los pacientes** en los sistemas de HME es de vital importancia. Si se utilizaran datos de una persona distinta debido a la identificación incorrecta de un paciente, las consecuencias en muchos casos serían nefastas.

Las tarjetas sanitarias emitidas en tarjetas inteligentes podrían contribuir considerablemente a una identificación electrónica adecuada de los pacientes, y también a su **autenticación**[21] **para acceder a sus propios datos del HME.**

b) Por otra parte, habida cuenta de la especial sensibilidad de los datos sobre la salud, es imperativo que no sea posible el acceso de personas no autorizadas. Un control fiable del acceso depende de una identificación[22] y una autenticación fiables. Esto hace necesario **identificar de forma única y autenticar correctamente a los usuarios**[23]**.**

Puesto que una de las principales ventajas de los sistemas de HME es su disponibilidad para el acceso por vía electrónica con independencia de la hora y la localización, será necesario establecer unas rutinas para la identificación y autenticación electrónicas fiables. La autenticación mediante la firma electrónica, que se concede a usuarios autorizados junto con una identificación oficial adecuada, por ejemplo en tarjetas inteligentes especiales, debe preverse al menos en una perspectiva a más largo plazo, a fin de evitar los riesgos conocidos de la autenticación mediante contraseña.

Para los profesionales de la salud será necesario desarrollar un sistema de identificación y autenticación, que pruebe no sólo la identidad, sino también **la calidad en que actúa electrónicamente**, por ejemplo, como psiquiatra o como enfermera.

3. Autorización para acceder a los HME a efectos de lectura y escritura

a) Garantías generales relativas al acceso

Los datos contenidos en los sistemas de HME son historiales médicos confidenciales. Por tanto, el **principio esencial** relativo al acceso a un HME debe ser que, aparte del propio paciente, **sólo podrán tener acceso al mismo aquellos profesionales de la salud**/personal autorizado de instituciones sanitarias **que participen en ese momento en el tratamiento del paciente**. Debe existir una relación de tratamiento médico real y actual entre el paciente y el profesional de la salud que desee acceder a su HME.

Parece también necesario regular qué categorías de profesionales sanitarios/instituciones y a qué nivel pueden acceder a datos de los HME (¿médicos generalistas, médicos de hospital, farmacéuticos, enfermeras, quiroprácticos? ¿psicólogos? ¿terapeutas familiares? etc.).

La protección de los datos podría asimismo verse reforzada mediante unos **derechos de acceso modulares**, esto es, creando en un sistema de HME categorías de datos médicos de

---

[20] La "identificación" significa que una persona queda descrita por identificadores como el nombre, la fecha de nacimiento, la dirección etc.; en el presente contexto habrá que certificar oficialmente esta descripción mediante una partida de nacimiento, un pasaporte, una tarjeta sanitaria, etc.

[21] La "autenticación" permite certificar que la persona que declara tener una identidad determinada es realmente tal persona. Esto suele hacerse presentando un documento oficial de identidad que contenga una foto (por ejemplo, un pasaporte) o, en el mundo electrónico, utilizando la firma electrónica.

[22] La "identificación fiable" no debería utilizar números de identificación, ampliamente utilizados en otros contextos, sin garantías específicas, a fin de evitar una interconectabilidad fácil (véase el artículo 8, apartado 7, de la Directiva).

[23] En Francia, los primeros experimentos que están a punto de comenzar con HME se basan en la creación de un identificador específico; todavía no es seguro si este sistema se mantendrá en la configuración final del sistema HME.

forma que el acceso esté limitado a categorías específicas de profesionales o instituciones sanitarias[24]. Las posibles ventajas de una configuración modular de los HME se tratarán más ampliamente en el punto 6.

b) Garantías especiales de acceso ques suponen la participación del paciente

Si es viable y posible, esto es, si está presente y es capaz de actuar, deberá **darse al paciente la facultad de impedir el acceso a sus datos del HME si lo desea**. Esto requiere que el paciente esté informado previamente de quién desea, cuándo y porqué acceder a sus datos, y acerca de las posibles consecuencias de no permitir el acceso. Es necesario desarrollar procedimientos que eviten que se ejerza una presión psicológica indebida sobre el paciente con el fin de que éste autorice el acceso a sus datos.

Cuando sea necesario **probar que el paciente ha dado su acuerdo** para que se acceda a los datos de su HME, será imprescindible contar con instrumentos fiables para tal prueba, como por ejemplo la comprobación electrónica de la ficha (*token*) del paciente, o, si tales instrumentos están ya generalizados, la firma electrónica del paciente, etc. La presentación de tal prueba deberá documentarse electrónicamente a efectos de una posible auditoría.

Deberán definirse normas que establezcan si el interesado puede exigir que determinados datos no se incorporen a su expediente. Una posible manera de resolver esta cuestión podrían ser los "sobres sellados", que no pueden abrirse sin el consentimiento explícito del interesado.

c) Acceso de los interesados a los datos de su propio HME

La cuestión de si debe concederse a los pacientes **acceso (electrónico) directo de lectura** a su propio HME es una cuestión de viabilidad médica. El derecho de acceso asociado a la protección de los datos, por ejemplo de conformidad con el artículo 12 de la Directiva 95/46/CE, no significa siempre necesariamente acceso *directo*. El acceso directo podría, sin embargo, contribuir considerablemente a la confianza en un sistema de HME. Desde el punto de vista de la protección de los datos, una condición previa para conceder el acceso directo sería la identificación y autenticación electrónica segura a fin de impedir el acceso de personas no autorizadas.

En las disposiciones que regulen el sistema de HME también debería abordarse la cuestión de si los **pacientes** deben **introducir ellos mismos datos en su HME** o si deben hacer que los introduzca un profesional de la salud. Los posibles problemas de responsabilidad por lo que respecta a la exactitud se resolverían probablemente con una transparencia adecuada de los procedimientos de codificación, que revelan al autor de las inscripciones en el HME. También se podría estudiar la posibilidad de limitar el acceso de escritura a un módulo especial dentro del HME.

En este contexto, deberán tenerse en cuenta las capacidades y necesidades especiales de los enfermos crónicos, los ancianos, los discapacitados y los minusválidos.

4. Uso de HME para otras finalidades

La aceptación de los sistemas de HME por los ciudadanos dependerá de su **confianza en la confidencialidad del sistema.**

La justificacion del acceso legítimo a los datos de un HME debe corresponder a la finalidad esencial de todo sistema de HME, es decir, realizar un buen tratamiento médico gracias a una mejor información. **El Grupo de Trabajo opina que debería prohibirse en principio el**

[24] Por ejemplo, el acceso a los datos relativos a un tratamiento psiquiátrico podría limitarse en un primer nivel a los psiquiatras; o podría hacerse accesible un módulo especial sobre medicación para los farmacéuticos, que no tienen acceso a otras partes de un sistema de HME.

acceso a los datos médicos de un HME con fines distintos de los mencionados en el artículo 8, apartado 3.

Esto excluiría, por ejemplo, el acceso a los HME de profesionales médicos que actúen como expertos para terceros: por ejemplo, para compañías de seguros privadas, en pleitos, para conceder ayudas a la jubilación, para los empleadores del interesado, etc. Además, la normativa disciplinaria aplicable a los profesionales sanitarios deberá prever sanciones eficaces en caso de violación de estas normas.

Deberán adoptarse medidas especiales para impedir que se induzca ilegalmente a los pacientes a revelar sus datos del HME, por ejemplo a petición de un posible futuro empleador o de una compañía de seguros privada. Es esencial que los pacientes estén informados para evitar que accedan a tales peticiones de comunicación, que serían ilegales conforme a la normativa sobre protección de datos. También deberán aplicarse medios técnicos, por ejemplo requisitos especiales para la impresión íntegra de un HME, etc.

El tratamiento de los datos de los HME a efectos **de estadísticas oficiales y de investigación médica y científica** podría permitirse como excepción a la regla establecida anteriormente**,** siempre que todas estas excepciones sean conformes con la Directiva (véase el artículo 8, apartado 4, y el correspondiente considerando 34): deberán estar por tanto previstas por la ley para fines previamente determinados y específicos, en condiciones especiales que garanticen la proporcionalidad ("garantías apropiadas y específicas"), con el fin de proteger los derechos fundamentales y el derecho a la intimidad de las personas.

Por otra parte, siempre que sea viable y posible, los datos de los sistemas de HME deberán utilizarse para otras finalidades (por ejemplo, estadísticas o control de calidad) sólo de forma anónima o al menos utilizando pseudónimos seguros[25].

5. Estructura organizativa de un sistema de HME

En el contexto del debate sobre las diversas alternativas de organización para almacenar datos en un sistema de HME, suelen mencionarse las siguientes alternativas principales:

- el HME como sistema que proporciona acceso a los historiales médicos que guarda el profesional de la salud, que tiene la obligación de conservar un historial sobre el tratamiento de sus pacientes. Esto suele denominarse **"almacenamiento descentralizado"**;
- el HME como sistema uniforme de almacenamiento, al que los profesionales médicos deben transferir su documentación; esto suele denominarse **"almacenamiento centralizado"**;
- una tercera alternativa puede ser permitir que el interesado sea "dueño" de sus propios historiales médicos, ofreciéndole **el almacenamiento de sus propios datos médicos como un servicio electrónico especial bajo su control**, e incluso dándole el poder de decidir los datos que deben figurar en el HME[26].

a) Mientras que la tercera alternativa **(almacenamiento bajo el control del interesado)** parece ser la mejor solución por lo que respecta a la autodeterminación, la calidad de esta

[25] La utilización de pseudónimos supone la transposición de identificadores (como nombres y fechas de nacimiento, etc.) bajo una nueva designación, preferiblemente mediante encriptación, de modo que el receptor de la información no pueda identificar al sujeto de los datos.

[26] Éste es el modelo francés que se está estableciendo actualmente. Los prestadores de servicios se denominan centrales ("hébergeurs") y su estatuto se regula mediante un decreto que fue objeto de un dictamen previo de la CNIL. Se trata de un sistema complejo y se basa en la acreditación de los prestadores de servicios y en la seguridad del sistema.

documentación por lo que respecta a la exactitud y amplitud pueden plantear problemas, si es únicamente el interesado quien decide qué datos se guardan en su HME y no se integra en el sistema ninguna intervención de un profesional médico.

b) En el caso del modelo de **almacenamiento "descentralizado"**, que sólo se convierte en un "sistema" a través de la creación de caminos de búsqueda, la estructura de documentación de los datos sanitarios de los distintos prestadores de servicios sanitarios no se modifica. La medida en que los datos de un paciente pueden localizarse en este sistema depende de la calidad del sistema de búsqueda.

En este modelo organizativo, el **profesional o la institución sanitaria es "responsable"** del expediente (o más concretamente, de la parte del HME creado por él). A la vista de la complejidad de la arquitectura de este modelo, podría ser necesario designar un organismo central encargado de gestionar y controlar todo el sistema, y también de garantizar su compatibilidad de la protección de los datos. También podría ser útil que los interesados pudieran someter sus problemas de protección de datos a un organismo central, en vez de tener que buscar entre una multitud de responsables.

c) La principal ventaja del llamado sistema de **almacenamiento "centralizado"** sería probablemente una mayor disponibilidad y seguridad técnica (acceso 24 horas), lo que no es tan fácil de garantizar si un sistema de HME se extiende más allá de los hospitales. Habrá un solo responsable para todo el sistema, independiente de los profesionales o instituciones sanitarias que hayan enviado su documentación (parcial o global) al sistema central.

Por lo que respecta a la protección de los datos, podrían formularse objeciones contra un sistema de este tipo, por lo que se refiere a la mayor posibilidad de uso ilícito del almacenamiento centralizado de datos. Podrían preverse disposiciones y medidas de seguridad especiales (por ejemplo, almacenamiento cifrado), a fin de compensar, al menos en gran parte, los riesgos de seguridad que plantea la centralización de los datos. Sin embargo, la responsabilidad de la confidencialidad escapa entonces a los profesionales médicos, lo que podría influir en la confianza de los pacientes en el sistema.

La medida en que el paciente puede influir en el contenido y la comunicación de su HME dependería en ambos casos - almacenamiento descentralizado y centralizado - de la configuración particular del sistema (véase el punto 3 b).

6. Categorías de datos almacenados en los HME y modos de presentación

La idea básica de un "sistema de HME" consiste en recoger todos los datos relativos a la salud de una persona concreta que puedan tener importancia para el estado de su salud a largo plazo, de modo que en caso de necesitarse tratamientos futuros se pueda contar con una información completa y pertinente, y los pacientes puedan beneficiarse de un mejor tratamiento.

El Grupo de Trabajo considera que esto puede dar lugar a los siguientes problemas principales:

a) La **"exhaustividad" de un expediente médico** es prácticamente imposible, y tampoco es deseable: **solamente debería introducirse en un HME la información *relevante***. Una de las cuestiones más difíciles a la hora de establecer un sistema de HME será por tanto decidir qué categorías de datos médicos deben recogerse en un HME y durante cuánto tiempo deben conservarse[27]. Si bien esta pregunta debe ser respondida por expertos médicos, también tiene

[27] Hay categorías de datos que son importantes a lo largo de toda la vida del paciente (por ejemplo, las alergias), pero también hay datos que son sumamente importantes sólo durante un breve periodo, como por ejemplo incompatibilidades de tratamientos.

una dimensión en materia de protección de datos: según los principios de pertinencia y proporcionalidad de la recopilación de datos, toda compilación de datos debe limitarse a aquellos datos que sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (artículo 6, apartado 1, letra c), de la Directiva). La legitimidad de los sistemas de HME también dependerá por tanto de una solución adecuada para elegir las categorías "adecuadas" de datos y la duración "adecuada" de almacenamiento de la información en un HME.

b) Por lo que respecta a la presentación de los datos en los HME: el hecho de que sea posible distinguir entre diversas categorías de datos sanitarios que requieren grados muy distintos de confidencialidad sugiere que podría ser útil en general crear distintos **módulos de datos** en un sistema de HME con distintos requisitos de acceso: un "módulo de datos de vacunación" debería estar accesible en cualquier momento para el interesado y podría también estar accesible para una gama bastante amplia de personal sanitario; podría existir un "módulo de datos de medicación", con acceso especial para farmacéuticos, si el paciente está de acuerdo[28]; un "módulo de datos de urgencia" podría contar con medios técnicos especiales de acceso, etc. La creación de módulos para "sistemas de recordatorio" especiales también podría tener sentido; servirían para recordar automáticamente a un paciente las vacunas, los chequeos y las revisiones necesarias.

Los datos particularmente sensibles podrían también protegerse mejor mediante su almacenamiento en módulos separados con condiciones de acceso especialmente estrictas. Como ejemplo cabe mencionar los datos sobre tratamientos psiquiátricos, VIH o abortos. En vez de excluir tales datos de un HME, lo que podría ser perjudicial para un correcto tratamiento médico futuro, deberían introducirse en el sistema restricciones especiales para el acceso a tales datos del HME, incluido el consentimiento explícito del paciente y barreras técnicas especiales (por ejemplo, "sobres sellados").

c) Al estructurar los historiales de HME, también deberán tenerse en cuenta las **demandas de información especiales** recurrentes. Un ejemplo: conforme al derecho nacional, las compañías de seguros privadas podrían tener derecho a recibir una cierta información (limitada) relativa a los historiales médicos, cuando ello sea necesario en el contexto del cumplimiento de sus obligaciones contractuales con respecto a los pacientes asegurados. El otorgar acceso a las compañías de seguros privadas al HME de un paciente parece inaceptable. Por esta razón, una solución podría ser crear un "paquete" especial estándar de "documentación" que, cuando sea necesario, resuelva los intereses legítimos de información del asegurador y que, si el paciente lo autoriza, podría transmitirse (electrónicamente) a la compañía de seguros privada.

7. Transferencia internacional de historiales médicos

La disponibilidad electrónica de datos médicos en los sistemas de HME puede mejorar considerablemente las facilidades de diagnóstico o de tratamiento, permitiendo el recurso a conocimientos médicos disponibles solamente en instituciones médicas extranjeras. La consulta de expertos extranjeros a efectos de diagnóstico no requiere generalmente que se revele la identidad del paciente. Por tanto, en la medida de lo posible, tales datos deberían transferirse a países fuera de la Unión Europea o del Espacio Económico Europeo de forma **anónima o al menos utilizando pseudónimos**. Si no se cuenta con el consentimiento explícito del interesado para la transferencia de datos personales[29], esta solución también

[28] La ventaja de incluir un módulo de medicación en el HME sería doble, porque también daría al médico la posibilidad de ver toda la medicación que toma el paciente.

[29] Cuando un paciente sea físicamente incapaz de responder a una solicitud de consentimiento (por ejemplo, si se encuentra en coma), sus datos médicos podrían no obstante, de conformidad con el artículo 26,

evitaría la necesidad de obtener permiso para esta transferencia de datos, pues el interesado no es identificable para el receptor de los mismos.

Teniendo en cuenta el elevado riesgo que existe para los datos personales contenidos en un sistema de HME en un medio sin protección adecuada, el Grupo de Trabajo del artículo 29 subraya que todo tratamiento – en especial el almacenamiento - de datos de los HME deberá realizarse en países que apliquen la Directiva de protección de datos de la UE o un marco jurídico adecuado de protección de datos.

Los intercambios de datos transfronterizos en el marco de estudios clínicos plantean un problema específico: el grupo de estudio que trata directamente con los pacientes puede necesitar a veces acceder a los datos de los HME en su forma personalizada original. No obstante, para todas las transferencias de datos resultantes de estudios clínicos a patrocinadores u otras instituciones legalmente implicadas, debe exigirse la utilización de pseudónimos seguros como requisito mínimo, en particular si tales patrocinadores se encuentran en países que no cuentan con una protección adecuada de los datos.

Especial atención debería prestarse siempre en este contexto a los aspectos de la seguridad de los datos, a fin de evitar riesgos de divulgación no autorizada en medios que posiblemente no sean seguros desde el punto de vista de la protección de los datos.

8. Seguridad de los datos

La aceptabilidad de un sistema de tratamiento de datos con un potencial de riesgo excepcional depende de la existencia de un nivel suficientemente elevado de seguridad de los datos en el conjunto del sistema. **El acceso por parte de personas no autorizadas debe ser virtualmente imposible y verse impedido** para que el sistema sea aceptable desde el punto de vista de la protección de datos. Sin embargo, el acceso de los profesionales autorizados en caso de necesidad real de esta información deberá ser prácticamente ilimitado, a fin de que el sistema proporcione los beneficios prometidos para el tratamiento médico de los pacientes.

El marco jurídico por el que se crea un sistema de HME debería prever la aplicación de una serie de medidas técnicas y organizativas destinadas a evitar la pérdida de datos o la alteración, tratamiento y acceso no autorizados a los datos en el sistema de HME. La integridad del sistema debe garantizarse haciendo uso de los conocimientos e instrumentos más avanzados en materia de informática y tecnología de la información.

Las tecnologías de protección de la intimidad (PET)[30] deberán aplicarse en la medida de lo posible, a fin de promover la protección de los datos personales. La encriptación debería utilizarse no sólo para la transferencia, sino también para el almacenamiento de datos en los sistemas de HME. Todas las medidas de seguridad deberían ser de fácil utilización, a fin de generalizar su aplicación. Los costes correspondientes deberán considerarse como una inversión en la compatibilidad de los sistemas de HME con los derechos fundamentales, que será una de las condiciones más importantes para el éxito de estos sistemas.

Independientemente del hecho de que muchas de las garantías mencionadas contengan de por sí elementos de seguridad de los datos, el marco jurídico relativo a las medidas de seguridad debería prever especialmente la necesidad:

- de un sistema fiable y eficaz de identificación y autenticación electrónicas, así como de registros constantemente actualizados, que permitan comprobar si las personas que

apartado 1, letra e), de la Directiva, transferirse a países que no cuenten con una protección adecuada de los datos, si sus intereses vitales así lo exigen.

[30] Por lo que respecta a las PET, véase el punto 4.3 del "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE)", de la Comisión, COM (2003) 265 final.

tienen o solicitan acceso al sistema de HME cuentan con la autorización necesaria;

- del registro y la documentación exhaustivas de todas las fases de tratamiento de datos que se realicen en el sistema, especialmente las solicitudes de acceso de lectura o escritura, junto con controles internos regulares y el control de la autenticidad de la autorización;
- de mecanismos eficaces de copia de seguridad y de recuperación destinados a proteger el contenido del sistema;
- de la imposibilidad de acceso no autorizado o de alteración de los datos del HME en el momento de la transferencia o el almacenamiento de las copias de seguridad, por ejemplo mediante la utilización de algoritmos criptográficos;
- de instrucciones claras y documentadas a todo personal autorizado sobre cómo utilizar correctamente los sistemas de HME y cómo evitar riesgos y fallos de seguridad;
- de una distinción clara de las funciones y competencias por lo que respecta a las categorías de personas responsables del sistema o que participen en el mismo, a fin de poder determinar a los responsables en caso de problemas;
- de controles internos y externos regulares en materia de protección de datos.

9. Transparencia

Parece evidente que un HME ofrece grandes posibilidades para el tratamiento médico, pero en principio también presenta un riesgo elevado de uso ilícito mediante el acceso no autorizado. Para confiar en el sistema, la opinión pública y los individuos exigirán por tanto una mayor transparencia por lo que **respecta al contenido y el funcionamiento de un sistema de HME**. El responsable o responsables del sistema deberán efectuar la **notificación** a las autoridades responsables de la protección de datos, junto con una información **especial, fácilmente disponible y comprensible**. El uso de Internet como canal ideal de difusión de la información puede ayudar a crear la transparencia necesaria sobre los sistemas de HME establecidos en los distintos países.

Unos puntos de acceso gratuitos y fáciles de utilizar, pero seguros, para que los interesados puedan comprobar el contenido y la revelación de su historial HME, podrían ser también una contribución valiosa a la transparencia y por tanto a la confianza en el sistema.

10. Cuestiones relacionadas con la responsabilidad

Todo sistema de HME debe también garantizar que las **posibles violaciones de la intimidad** que causen el almacenamiento y el suministro de datos médicos en un sistema de HME se vean **adecuadamente compensadas mediante la responsabilidad por los daños** causados, por ejemplo, por el uso incorrecto o no autorizado de los datos de los HME.

El análisis de los posibles problemas que los sistemas de HME pueden ocasionar desde el punto de vista de la protección de datos sólo puede tratar superficialmente las cuestiones de responsabilidad por uso incorrecto de un sistema de HME. En opinión del Grupo de Trabajo, cualquier Estado miembro que desee introducir un sistema de HME deberá realizar previamente estudios jurídicos y médicos, así como evaluaciones de impacto, para aclarar las nuevas cuestiones en materia de responsabilidad que puedan surgir en este contexto, por ejemplo por lo que respecta a la exactitud y exhaustividad de los datos incorporados en los HME, por lo que respecta a la definición del grado de conocimiento que un profesional de la salud que trata a un paciente debe tener del HME, o por lo que respecta a las consecuencias previstas por la ley en caso de que el acceso no esté disponible por razones técnicas, etc.

11. Mecanismos de control del tratamiento de los datos contenidos en los HME

A la vista de la **situación especial de riesgo** que crea el establecimiento de los sistemas de HME, es necesario prever **mecanismos de control eficaces** para evaluar las garantías existentes. La complejidad de la información contenida en un HME, junto con la multitud de posibles usuarios, puede exigir nuevos procedimientos por lo que respecta a los derechos de acceso de los interesados:

a) Deberá establecerse **un procedimiento arbitral especial para los litigios** relativos al uso correcto de los datos en los sistemas de HME; los interesados deberán poder hacer uso de tal procedimiento de forma fácil y gratuita. Teniendo en cuenta que en la evaluación de las reclamaciones relativas a datos erróneos o tratados innecesariamente en los sistemas de HME generalmente se requerirán competencias médicas específicas, las autoridades nacionales de control de protección de los datos podrían no ser la mejor opción para tratar tales reclamaciones, al menos no en primera instancia. Los "defensores de los pacientes" podrían, en los casos en que ya existan, ser responsables de esta tarea.

b) Un sistema de HME debe permitir al interesado ejercer sus derechos de acceso sin dificultades indebidas. En principio, el responsable del tratamiento de datos está obligado a conceder el acceso. **Los sistemas de HME son**, sin embargo, **sistemas de puesta en común de información,** con muchos responsables distintos. En estos sistemas con un gran número de responsables del tratamiento de datos, **una única institución especial debe ser responsable, por lo que respecta a los interesados, de la correcta gestión de las solicitudes de acceso**. A la vista de la previsible complejidad de un HME totalmente desarrollado, y de la necesidad de ganar la confianza de los pacientes en el sistema, parece esencial que los pacientes cuyos datos se tratan en un sistema de HME sepan cómo ponerse en contacto con un socio responsable con quien puedan discutir posibles deficiencias del sistema de HME. Deberán incluirse disposicioens especiales a este respecto en las normas relativas a los sistemas de HME.

c) A fin de suscitar la confianza, podría introducirse **un procedimiento especial para informar a los interesados acerca de cuándo y quién ha accedido a sus HME**. El suministro a intervalos regulares a los interesados de una lista de las personas o instituciones que han accedido a su expediente tranquilizaría a los pacientes por lo que respecta a su capacidad de saber lo que sucede con sus datos en el sistema de HME.

d) Deberán realizarse **controles internos y externos regulares de los protocolos de acceso**. El mencionado informe anual sobre el acceso, enviado a los interesados, constituiría un medio efectivo adicional de comprobar la legalidad del uso de los datos de los HME. La designación de agentes encargados de la protección de datos en los hospitales que participan en los sistemas de HME mejorarían ciertamente la probabilidad de un uso correcto de los datos contenidos en estos sistemas.

IV. CONCLUSIÓN

Todos los individuos y todos los pacientes tienen derecho a la intimidad y pueden esperar de manera razonable que la confidencialidad y la protección de su información personal serán rigurosamente respetadas por todos los profesionales sanitarios. Esta expectativa es también válida por lo que se refiere a los sistemas de historiales médicos electrónicos (HME).

El Grupo de Trabajo del artículo 29 ha elaborado el presente documento de trabajo con el fin de proporcionar una orientación para la interpretación del marco jurídico de protección de datos aplicable a los sistemas de historiales médicos electrónicos (HME), y para establecer

algunos principios generales. El documento de trabajo también aspira a exponer las condiciones previas de protección de datos necesarias para el establecimiento de un sistema nacional de HME, así como las garantías aplicables, y a contribuir a la aplicación uniforme de las medidas nacionales adoptadas conforme a la Directiva 95/46/CE.

El Grupo de Trabajo del artículo 29 pone de relieve que el establecimiento y el funcionamiento de los sistemas HME deben respetar plenamente los principios de protección de los datos personales consagrados en la Directiva 95/46/CE. Considera que el cumplimiento de estos principios ayuda a todas las personas e instituciones implicadas a asegurar el funcionamiento adecuado de tales sistemas. Además, el Grupo de Trabajo del artículo 29 resalta la necesidad de crear y gestionar los sistemas de HME en un marco jurídico sólido con garantías dirigidas a proteger los datos personales, con independencia de cual sea la base jurídica de tales sistemas.

El Grupo de Trabajo del artículo 29 invita a la profesión médica, a los demás profesionales sanitarios y a las personas e instituciones que intervienen en la prestación de servicios médicos, así como al público en general, a que presenten comentarios sobre este documento de trabajo.[31]

Habida cuenta de la evolución continua en este ámbito, podría ser necesario realizar trabajos ulteriores, comentarios adicionales y un seguimiento por parte del Grupo de Trabajo del artículo 29.

Hecho en Bruselas, el 15 de febrero de 2007.

Por el Grupo de Trabajo
El Presidente
Peter SCHAAR

[31] Los comentarios a este documento de trabajo deben enviarse a:
Secretaría del Grupo de Trabajo del artículo 29
Comisión Europea, Dirección General de Justicia, Libertad y Seguridad
Unidad C.5 - Protección de datos personales
Despacho: LX 46 1/43
B - 1049 Bruselas
E-mail: Amanda.JOYCE-VENNARD@ec.europa.eu; Fax: + 32-2-299 80 94
Todos los comentarios tanto de los sectores públicos como privados se publicarán en el sitio de Internet del Grupo de Trabajo del artículo 29, a menos que los autores indiquen explícitamente que determinadas informaciones son confidenciales.