Informe 0411/2009

La consulta plantea la posibilidad de incorporar y alojar los datos resultantes de las acciones de vigilancia periódica de la salud de los trabajadores de sus empresas clientes, obtenidos por la consultante como empresa que presta el servicio de prevención de riesgos laborales, en una aplicación informática propiedad de la empresa cliente, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y en el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de dicha Ley.

I

Como cuestión previa conviene aclarar que en los términos previstos por la Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales, la misma tiene por objeto la determinación del cuerpo básico de garantías y responsabilidades necesarias para establecer un adecuado nivel de protección de las salud de los trabajadores frente a los riesgos derivados de las condiciones de trabajo, a partir del reconocimiento del derecho de los trabajadores en el ámbito laboral a la protección de su salud e integridad (articulo 2).

En cumplimiento del deber de protección, la Ley 31/1995 establece como obligación de la empresa, la de constituir un servicio de prevención que se responsabilice de las actividades de prevención y protección de riesgos laborales. Para la realización de dicha actividad deberá contar bien con un servicio de prevención propio o contratar con un servicio de prevención ajeno debidamente acreditado (artículo 14.2).

Atendiendo a lo que acabamos de indicar y en relación con el acceso a determinados datos de carácter personal relacionados con la salud de los trabajadores por parte de los empresarios, de cara a la aplicación de la normativa sobre protección de datos de carácter personal, la comunicación de los datos de salud resultantes de las revisiones médicas de prevención y vigilancia de la salud que efectuaría la empresa consultante prestadora del servicio de prevención de riesgos laborales a la empresa a la que pertenecen los trabajadores, constituye en principio un supuesto de cesión o comunicación de datos.

La cesión o comunicación de datos aparece definida en el artículo 3 i) de la Ley 15/1999 como “Toda revelación de datos realizada a una persona distinta del interesado”.

En lo que se refiere a la cesión de los datos de salud de los trabajadores al empresario, debemos señalar que, estos datos, dentro de los de carácter personal, tienen un régimen jurídico especial de protección. Ello tiene reflejo en el artículo 7. 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Persona, relativo a los datos especialmente protegidos, que indica: "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".

En este sentido, la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales establece en su artículo 22, relativo a la obligación por parte del empresario de garantizar la vigilancia de la salud a los trabajadores, lo siguiente:

"1. El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo.

Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad.

En todo caso se deberá optar por la realización de aquellos reconocimientos o pruebas que causen las menores molestias al trabajador y que sean proporcionales al riesgo.

2. Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud.

3. Los resultados de la vigilancia a que se refiere el apartado anterior serán comunicados a los trabajadores afectados.

4. Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador.

El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.

No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con

la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva.

5. En los supuestos en que la naturaleza de los riesgos inherentes al trabajo lo haga necesario, el derecho de los trabajadores a la vigilancia periódica de su estado de salud deberá ser prolongado más allá de la finalización de la relación laboral, en los términos que reglamentariamente se determinen.

6. Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada".

Este régimen legal específico del tratamiento de la salud en el ámbito laboral establece expresamente el carácter voluntario de las actividades de control periódico de la salud de los trabajadores (con la única excepción contemplada en el apartado primero del artículo transcrito), estableciendo también de forma expresa, la obligación de respeto a la intimidad de los trabajadores y de la confidencialidad de los datos.

En consecuencia, el acceso por parte del propio empresario al historial médico generado como consecuencia de los reconocimientos médicos realizados a los trabajadores deberá limitarse a las previsiones del artículo 22.4 que se citaba. En este sentido, se prohíbe la transmisión de la información médica obtenida al amparo de lo dispuesto en la Ley de Prevención de Riesgos Laborales a cualquier tercero distinto del "personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores", con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva.

II

Por otra parte, el artículo 23 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales señala, "1. El empresario deberá elaborar y conservar a disposición de la autoridad laboral la siguiente documentación relativa a las obligaciones establecidas en los artículos anteriores:

a) (….)

d) Práctica de los controles del estado de salud de los trabajadores previstos en el artículo 22 de esta Ley y conclusiones obtenidas de los mismos en los términos recogidos en el último párrafo del apartado 4 del citado artículo.

2. En el momento de cesación de su actividad, las empresas deberán remitir a la autoridad laboral la documentación señalada en el apartado anterior.

4. La documentación a que se hace referencia en el presente artículo deberá también ser puesta a disposición de las autoridades sanitarias al objeto de que éstas puedan cumplir con lo dispuesto en el artículo 10 de la presente Ley y en el artículo 21 de la Ley 14/1986, de 25 de abril General de Sanidad."

Por consiguiente, existirá también una habilitación legal para la cesión de datos de salud referidos a tales controles de salud a los trabajadores sin su consentimiento, a la autoridad laboral y autoridades sanitarias en el supuesto del cumplimiento de las obligaciones establecidas en el artículo 23 de la Ley 31/1995 y en los términos del artículo 22.4.

En consecuencia, como punto de partida, se prohíbe la transmisión de la información médica obtenida al amparo de lo dispuesto en la Ley de Prevención de Riesgos Laborales a cualquier tercero distinto del "personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores", incluido el profesional médico de la empresa en que los trabajadores prestan su actividad si no han efectuado la acciones de vigilancia de la salud de los trabajadores como es el caso, con la única excepción de las conclusiones derivadas de dicho seguimiento en cuanto a la aptitud de los trabajadores (artículo 22.4, párrafo tercero).

Por ello, no cabe entender amparada en la Ley 31/1995 ninguna cesión de datos, debiendo plantearse si existe algún supuesto en que la propia Ley Orgánica 15/1999 da cobertura a dicha cesión.

III

Al respecto, el párrafo primero del artículo 7.6 de la LOPD establece: "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".

Por su parte, el artículo 11.2.f), en su inciso primero, habilita la cesión de los datos "cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero".

De la lectura de ambos preceptos se desprende que la cesión deberá fundarse en que haya quedado debidamente justificada una necesidad de acceso a los datos específicos relacionados con la consulta efectuada en cada

caso concreto y siempre que sea necesaria para solucionar una urgencia del trabajador afectado. En este sentido, la Directiva 95/46/CE habilita la cesión de los datos fundada en la existencia de una urgencia vital para el afectado.

IV

Señala la consultante que los datos médicos obtenidos de tales reconocimientos se incorporarían a una base de datos informática propiedad de la empresa a la que pertenecen los trabajadores examinados, si bien, a dicha base sólo tendrían clave de acceso el personal médico que realizó dichos controles, las autoridades sanitarias y los empleados de la empresa cliente a cargo del mantenimiento de dicha base informática.

El supuesto descrito no dejaría de ser una comunicación por medios electrónicos de los datos de salud de los trabajadores al empresario y alcanzaría al conjunto de datos resultantes de los reconocimientos y pruebas clínicas realizadas por los profesionales sanitarios del servicio de prevención de riesgos laborales concertado con la Mutua consultante, por cuanto dichos datos aparecerían incorporados al sistema informático controlado por la propia empresa y, por consiguiente, accesible a ésta a través de las claves que la misma habilitara, excediendo esta posibilidad la habilitación del artículo 22.4 de la Ley 31/1995 analizada.

No obstante, si se pretende entablar con la empresa cliente un acuerdo de alojamiento de datos a modo de hosting en los servidores de ésta, tal posibilidad deberá enmarcarse en la figura del encargado del tratamiento de datos por cuenta de terceros regulada en el artículo 12 de la LOPD cuyas características son:

a) En primer lugar, será preciso que la actuación del encargado del tratamiento se limite a la prestación de los servicios objeto de la contratación. A tal efecto dispone el artículo 20.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999 que “se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado”.

b) En lo que atañe a los requisitos formales, el artículo 12.2 de la Ley Orgánica impone que “la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”.

c) Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que “una vez cumplida la prestación contractual, los

datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

Añade el artículo 20.3 del Reglamento que "no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo". El artículo 22.1 reitera esta previsión, al indicar que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

d) Por otra parte, a fin de preservar los derechos del encargado frente a posibles responsabilidades derivadas de su actuación, dispone el artículo 22.1 del Reglamento que "el encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".

e) En lo referente a la posible subcontratación de los servicios prestados, el artículo 21 del Reglamento permite esta posibilidad en caso de que el responsable del fichero apodere al encargado para la celebración del segundo contrato en nombre de aquél o cuando se den los requisitos especificados en el apartado 2 del citado precepto:

- "Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar". SI dicha circunstancia no se hubiera previsto en el contrato, deberá procederse a su modificación posterior, conforme al artículo 22.3. Igualmente, en caso de que en el contrato no conste la identificación de la empresa subcontratista "será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación".

- "Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero".

- Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato previsto en el artículo 12 de la Ley Orgánica.

f) En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la

Ley Orgánica, detallando el artículo 81 del Reglamento el modo en que deberán implantarse las medidas.

g) Por último, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen".

V

Ahora bien, en cuanto al almacenamiento y custodia de las historias clínicas resultantes de los reconocimientos practicados a los trabajadores por el servicio de prevención de la Mutua consultante, debe tenerse en cuenta que el centro o profesionales sanitarios que hubieren efectuado los mismos, como destinatarios de los datos de salud recabados a los trabajadores, vienen obligados a archivar, elaborar y custodiar la historia clínica resultante de acuerdo con lo dispuesto en los artículos 14 y 17 de 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, que dicen:

Artículo 14: "Cada centro archivará las historias clínicas de sus pacientes, cualquiera que fuera el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizados su seguridad, su correcta conservación y la recuperación de la información."

Añadiendo el artículo 17:

"1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

3. Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada y secuencial del proceso asistencial de los pacientes.

4. La gestión de la historia clínica por los centros con pacientes hospitalizados, o por los que atiendan a un número suficiente de pacientes bajo cualquier otra modalidad asistencial, según el criterio de los servicios de salud, se realizará a través de la unidad de admisión y documentación clínica, encargada de integrar en un solo archivo las historias clínicas. La custodia de dichas historias clínicas estará bajo la responsabilidad de la dirección del centro sanitario.

5. Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen.

6. Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley 15/1999, de Protección de Datos de Carácter personal."

De lo anterior se desprende que encargar el alojamiento de las historias clínicas (contrato de hosting) a terceros ajenos al propio centro o profesional sanitario que practicó los controles de salud, no eximiría a éstos del cumplimiento de la obligación de custodia, conservación y archivo señaladas por dichos artículos 14 y 17 de la Ley 41/2002. y del cumplimiento de las medidas de seguridad de nivel alto en sus sistemas de archivo e información, conforme exige el artículo 81. 3 a) del Reglamento, descritas detalladamente en los artículos 89 a 103 de esta norma, destacando las señaladas en los artículos 93 y 103 que dicen:

Artículo 93 : " 1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

Artículo 103 : "1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.(..)".

Y además, para el caso de que se procediera al encargo de tratamiento (alojamiento de los datos de salud de los trabajadores), con la empresa cliente de la Mutua y prestadora de este servicio, ésta vendría obligada al cumplimiento de las mismas medidas de seguridad que el responsable de los ficheros, como ya se señaló, debiendo elaborar un documento de seguridad en los términos exigidos por el artículo 88 del Reglamento, o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a

implementar en relación con dicho tratamiento (artículo 82.2) y el resto de las medidas de seguridad establecidas por el Reglamento (artículo 82.3).

Todo ello en aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal,