Informe 0501/2009

La consulta plantea diversas dudas en relación con las medidas de seguridad a adoptar para la instalación de una solución hardware/software diseñada para su uso en hospitales. Según señala el consultante se trata de una pantalla monitor, situada en cada una de las camas del centro hospitalario, a través de la cual el personal sanitario puede registrar las distintas constantes tomadas a los pacientes.

La primera de las cuestiones a examinar es la relativa a la forma de acceso a datos del paciente desde los paneles por el personal sanitario, que se efectuaría según se indica en la consulta mediante un lector del código de barras que se encuentra en la tarjeta identificativa del personal hospitalario e identifica de forma unívoca al profesional.

El Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse según la naturaleza de los datos a tratar el nivel correspondiente.

En lo que se refiere a la determinación de los niveles de seguridad establece el artículo 81.3 del citado Reglamento que "*Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:*

a. *Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual."*

Debe tenerse presente, además, que como señala dicho precepto, las medidas de seguridad tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

De esta manera, el artículo 91 del Reglamento impone en los ficheros de nivel básico como una de las medidas de seguridad la del control de acceso, disponiendo en su número primero que "*Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones",* para ello exige en su número tercero que *"El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados."*

Asimismo, establece una obligación de identificación y autenticación de los usuarios, exigiéndose ya desde el nivel básico una identificación

personalizada de los usuarios. Dispone el artículo 93.1, a estos efectos, que "*El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios*." Por su parte, el número 2 del mismo artículo prevé que "*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."*

En el nivel medio, esta medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la contenida en el artículo 98 según el cual "*El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."*

Por último, en el nivel alto, se requiere ya un registro de cada intento de acceso que se produzca, establece el artículo 103.1 que "*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*." Mientras que el número segundo del mismo artículo dispone "*En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido."*

Por consiguiente, además de la identificación inequívoca y personalizada del usuario autorizado, y la limitación del intento de accesos a que se refiere el artículo 98 se requiere la existencia de un registro de accesos en los términos establecidos en el artículo 103, cuya función es determinar quien ha intentado acceder a un determinado fichero en cada momento, si ha sido autorizado para ello, y en su caso, cual es el registro accedido.

En cuanto a la segunda cuestión planteada, debe indicarse que la visualización de los datos por personas diferentes al personal sanitario que pudieran encontrarse en la habitación del paciente cuando se accede a los datos, constituiría una cesión de datos definida en el artículo 3 de la Ley Orgánica 15/1999 como "*Toda revelación de datos realizada a una persona distinta del interesado."*

Tratándose, además, de datos de salud, es preciso indicar que el régimen establecido con carácter general para el tratamiento y cesión de datos personales en los artículos 6 y 11 de la Ley Orgánica 15/1999, se encuentra, por vía de excepción, sometido a particulares restricciones en lo que a los datos de salud respecta, por el artículo 7 de la citada Ley Orgánica, que establece en su número 3 la regla general de que *"los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".* Esta regla únicamente es matizada por la Ley Orgánica en sus artículos 7.6 y 8.

El artículo 7.6 establece en su párrafo primero que "*podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3* (datos de salud) *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".*

Asimismo, el artículo 8 de la Ley Orgánica 15/1999 dispone respecto a los datos de salud que "*Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad".*

Por consiguiente, las medidas indicadas en la consulta para evitar la visualización de los datos de salud del paciente por personas distintas al personal sanitario, resultan adecuadas a la finalidad perseguida, impidiéndose así que se produzca una cesión de datos sin el pertinente consentimiento del afectado.