Revista CESCO de Derecho de Consumo **Nº 8/2013**

http://www.revista.uclm.es/index.php/cesco **I. Estudios y Consultas**

PROTECCIÓN DE DATOS SANITARIOS: LA HISTORIA CLÍNICA Y SUS ACCESOS

Igor Pinedo García
Abogado de ASJUSA LETRAMED

Resumen: Estudio sobre la protección de datos sanitarios, describiendo el uso y tratamiento de la Historia Clínica asistencial, analizando los distintos accesos que se llevan a cabo sobre la misma en diferentes áreas sanitarias.

Palabras clave: Protección de datos sanitarios, Historia Clínica, registro de accesos.

Title: Health Protection of Personal Data: the Medical Report and their access

Abstract: Overview of the Spanish legislation about Health Protection of Personal Data and the variety of different access respect to the medical records of patients.

Key words: Health Protection of Personal Data, the Medical Records, register of access.

1. Introducción

De acuerdo con nuestra actual normativa legal, el documento de Historia Clínica se configura como un instrumento capital, al objeto no sólo de probar una correcta o incorrecta praxis médica, sino de acreditar, en su caso, una vulneración de derechos fundamentales reconocidos por la Constitución Española[1].

[1] Art. 18.1 Constitución Española :
"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

La Historia Clínica viene definida y regulada, en cuanto su contenido y tratamiento se refiere, en la Ley 41/2002, de 14 de noviembre, reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica (LAP), toda vez que trata con profundidad todo lo referente a la documentación clínica generada en los centros asistenciales, subrayando especialmente la consideración y la concreción de los derechos de los usuarios en este aspecto. Conforme a dicha norma, la Historia Clinica se define como el conjunto de documentos que contienen datos, valoraciones e información de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial. Por "documento", la citada norma entiende cualquier tipo o clase de soporte que contenga un conjunto de datos e informaciones de carácter asistencial[2].

Sin embargo, a pesar de que la asistencia sanitaria al paciente constituye la causa y fin de la creación, mantenimiento y conservación de la Historia Clinica, no es, sin embargo, la única, toda vez que la misma despliega su eficacia en los ámbitos de gestión y organización, inspección médica, investigación, docencia, planificación sanitaria, y judicial (en este ámbito, especialmente con carácter probatorio)[3].

Por ello, la disparidad de tratamientos de una Historia Clínica, mas allá de la meramente asistencial, motivó que con la aprobación de la citada LAP se regulará de forma expresa aquellos requisitos necesarios para llevar a efecto tratamientos con fines judiciales, docentes o de investigación médica entre otros[4], obligándose para tales fines al cumplimiento expreso de la normativa en materia de Protección de Datos de Carácter Personal.

Esta remisión legal expresa, deviene como consecuencia del tipo de información que la Historia Clinica contiene. Un tipo de información, que de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), constituye información especialmente protegida[5], dado que se trata de datos de salud de las personas; las consecuencias de una disposición arbitraria y discrecional de la misma sin el consentimiento expreso del propio paciente o sin habilitación legal en su defecto, puede conllevar, no sólo la pertinente sanción para su autor, sino a sufrir importantes consecuencias en la esfera íntima de la propia persona titular de dicha información. Así, el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter

[2] Art. 3 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 (LAP)

[3]. MÉJICA GARCIA, JUAN M. *La Historia Clinica: Estatuto Básico y Propuesta de Regulación*. Ed. Edisofer. Madrid. 2002. P.21

[4] Art. 16.3 LAP: "*El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso*."

[5] Art. 7.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD):"*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"*

clínico-asistencial, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de dichos datos, en los cuales habrá que estar a los que dispongan los Jueces y Tribunales en el proceso correspondiente[6].

Sin embargo, a pesar de las distintas disposiciones normativas en este sentido, tanto en la práctica clínica habitual como en la propia gestión sanitaria, son frecuentes los casos en los que se producen intromisiones y tratamientos ilegítimos de esta información reservada, bien por destinar la misma a usos no consentidos por el paciente[7], o bien por dar accesos a personas no autorizadas para el mismo[8].

Por ello, los derechos a la protección de la intimidad personal y protección de datos de carácter personal persiguen garantizar a sus titulares un poder de control sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, pudiendo resguardar su vida privada de una publicidad no querida, garantizando a los individuos un poder de disposición sobre sus datos[9].

Al margen de la exhaustiva normativa reguladora existente en esta materia, la complejidad y especialidad de este tipo de documento (Historia Clinica) como la del propio sistema sanitario en sí mismo, dificultan sobremanera la capacidad probatoria de los pacientes en la evidencia de los filtros y autoría de estas intromisiones ilegitimas que atentan contra el derecho y libertades fundamentales. A esta dificultad contribuye sobremanera la Sociedad de la Información en la que vivimos; si bien uno de los mayores desafíos a los que se enfrenta el Sistema Nacional de Salud en la actualidad es el de la Historia Clínica Electrónica, no es menos cierto que lo mismo constituye una realidad que empieza a consolidarse dentro del panorama hospitalario a nivel global. Esta implantación implica una estructuración y organización que dificulta la

[6] Art. 16.3 LAP

[7] STS, Sala de lo Civil, 27 de enero de 1997 (RJ 1997\21): *"En el caso, se ejercita acción de responsabilidad por culpa extracontractual, con apoyo en los artículos 1902 y 1903 del Código Civil contra el Hospital xxxxxxxxx (Comunidad Autónoma de xxxxxxx) en reclamación de cantidad indemnizatoria por los daños y perjuicios experimentados por el actor, hoy parte recurrida, como consecuencia de la falta de atención y cuidado en la guarda y custodia, por los empleados del centro hospitalario demandado, de su historia clínica con motivo de su ingreso en el mismo para ser operado de un neuroma y en la que constaba que padecía el síndrome de inmunodeficiencia adquirida -Sida- y que dio lugar a su conocimiento por terceras personas extrañas, que han querido chantajearle y que han remitido fotocopia de la misma al colegio donde cursan sus estudios los hijos de aquél."*

[8] STC, Sala Primera,14 de febrero de 1992 (RTC 1992\20): *"(…) la identificación periodística (...) de una determinada persona, como afectada por el Síndrome de Inmunodeficiencia Adquirida (SIDA), deparaba, teniendo en cuenta actitudes sociales que son hechos notorios, un daño moral (y también económico como luego se demostró) a quienes así se vieron señalados como afectados por una enfermedad cuyas causas y vías de propagación han generado y generan una alarma social con frecuencia acompañada de reacciones, tan reprochables como desgraciadamente reales, de marginación para muchas de sus víctimas."*

[9] STC, Sala Pleno, 30 de noviembre de 2000 (RTC 2000\292): **"***La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad"*

adquisición de pruebas al ciudadano para poder plantear cualquier tipo de reclamación en este sentido.

2. Los formatos de la historia clínica

Inmersos en la Sociedad de la Información, el trasvase o cambio de formato en la configuración e instrumentalización de la historia clínica es una consecuencia obvia de este proceso de integración tecnológica. La optimización de recursos y mejora de la gestión y calidad asistencial, la posibilidad de acceso a toda la información clínica de un paciente en cada momento, impedir la pérdida de información de los pacientes, la disminución del margen de errores y facilitar el acceso a la información constituyen algunos de los motivos que han justificado este cambio de formato (papel – electrónico). No obstante, la consecución de tales propósitos puede, en ocasiones, transgredir los principios de calidad, información y consentimiento reconocidos por la normativa reguladora de la protección datos de carácter personal.

Este proceso de adaptación de los centros sanitarios a las directrices de la Sociedad de la Información, a pesar de ser lento, constituye ya una realidad. No obstante, a pesar de la consolidación del formato electrónico en el manejo de historiales clínicos, el soporte manual todavía se encuentra presente, de forma compartida, en multitud de centros sanitarios. Esta dualidad, existente en gran número de centros sanitarios, debe de provocar en los responsables de la gestión y tratamiento de la documentación clínica, un respeto más exigente de las directrices publicadas en materia de protección de la información clínica. Esta dualidad implica una doble obligación de seguridad por parte de los responsables de la guarda y custodia de esta información; doble obligación que se traduce en la adopción de las medidas de seguridad que dispone el Real de Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (RD 1720/2007), tanto en la gestión de los historiales clínicos en soporte papel, como en la configuración y administración de un sistema de Historia Clínica Electrónica.[10]

En cualquier fase del tratamiento, las personas que utilizan los datos de carácter personal están obligadas al secreto profesional, es decir, no podrán revelar la información a terceros sin el consentimiento expreso del afectado o sin habilitación legal al efecto. Debe de tenerse en cuenta que la obligación de secreto afecta a cualquier personal que intervenga en el tratamiento de los datos de carácter personal, no limitándose a aquellas personas que por el ejercicio de una determinada actividad estén sujetos al secreto profesional. Este deber de secreto subsiste incluso después de haber terminado la relación

[10] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. *"Seguridad y Protección de Datos Personales".* Ed. Thomson – Civitas. 2009. p. 57:
"Son un tipo de fichero que mezcla un acceso informatizado, e, incluso, una grabación informatizada de una parte de los datos, con un almacenamiento de datos en soportes no informáticos. Por ejemplo, un fichero de datos que contuviese una parte de sus datos en microfilms, cintas de audio, manuscritos, etc, es decir, soportes no informatizados, junto con otros datos informatizados, o un fichero manual con un índice informatizado para su acceso. (…) La legislación aplicable a este tipo de ficheros es la propia de los ficheros automatizados y la de los manuales, cada una aplicada a la parte del fichero correspondiente."

laboral, administrativa o de cualquier otra índole que se mantenga con el responsable de la información. Este deber de secreto debe de ser conocido por todas las personas de la organización que tratan o utilizan datos de carácter personal. Se trata de un deber distinto del que ya de por sí tienen algunos profesionales concretos (médicos, asistentes sociales, etc.) y que en el caso de estos profesionales concurre con aquél.[11] Los datos contenidos en la Historia Clínica son por sí mismos capaces de producir el perjuicio típico, por lo que el acceso a los mismos, su apoderamiento o divulgación, poniéndolos al descubierto, comporta ya un daño al derecho de mantenerlos secretos u ocultos[12].

2.1. Medidas de Seguridad en la gestión de Historias Clínicas. Infracción del deber de secreto

Como se ha expuesto, la dualidad entre historias clínicas en formato electrónico e historias clínicas en formato papel, obliga a la adopción de medidas de seguridad independientes respecto a la información tratada en uno u otro formato.

En este sentido, y por lo que al soporte papel se refiere, uno de los protagonistas sobre los que recae una misión trascendental de controlar los distintos historiales clínicos, es la Unidad de Archivo y Documentación Clinica del centro sanitario correspondiente.

2.1.1. Registro de Accesos

En lo que se refiere al tratamiento de historias clínicas en soporte papel, el RD 1720/2007 obliga a los centros responsables de esta documentación, a la implementación de una serie de medidas de seguridad que, además de pretender evitar accesos no autorizados, puedan orientar, llegado el momento, al origen de un acceso o tratamiento de información ilegítimo. Dichas medidas de seguridad se concretan en el establecimiento de un sistema y registro de accesos a la documentación clínica, en donde su acceso se limite exclusivamente al personal autorizado, en donde se implanten mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios y que, en los casos en los que se acceda a la Historia Clinica por personal no autorizado a priori, dichos accesos

[11] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. *Protección de datos personales para Servicios Sanitarios Públicos*. Ed. Thomson – Civitas. 2008. pp 191-191

[12] STS, Sala de lo Penal, 30 de diciembre de 2009 (RJ 2010\437): *"Y en cuanto a la distinción entre datos "sensibles" y los que no lo son, debe hacerse en el sentido de que los primeros son por sí mismos capaces para producir el perjuicio típico, por lo que el acceso a los mismos, su apoderamiento o divulgación, poniéndolos al descubierto comporta ya ese daño a su derecho a mantenerlos secretos u ocultos (intimidad) integrando el "perjuicio" exigido, mientras que en los datos "no sensibles", (…) debería acreditarse su efectiva concurrencia y en el caso presente, no se ha acreditado -ni se ha articulado prueba en este sentido- de que el acceso por parte del recurrente al nombre del médico cabecera -dato administrativo, y en principio, inocuo- del Dr.XXXXXXXX haya ocasionado perjuicio a éste como titular de al dato."*

queden debidamente registrados conforme al procedimiento que deba establecerse en el Documento de Seguridad del Centro. Por ello, si la finalidad del acceso de un profesional a la Historia Clínica es asistencial, este no puede acceder a la Historia Clínica de un paciente para identificar a un familiar con el que ha tenido un altercado en el aparcamiento del Hospital para poder presentar una denuncia[13].

Esta obligación en el registro de accesos viene igualmente impuesta para las historias clínicas gestionadas de forma automatizada o electrónica. El Real Decreto 1720/2007, dispone al efecto 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, así como que en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido. La identidad de la persona que haya accedido al contenido del historial clínico quedará desvelada por el usuario y contraseña que de forma obligada habrán de disponer los profesionales sanitarios autorizados para la lectura, modificación o ambas, de los historiales clínicos del Centro[14].

Sin embargo, uno de los inconvenientes de este último tipo de sistema de acceso (usuario y contraseña), es la propia memoria de la persona autorizada. Contraseñas complicadas o no basadas en alguna regla nemotécnica conducen a paradojas como que, si una contraseña es fácil de recordar para el usuario, será, a su vez, más fácil de descubrir por un atacante, y si es enrevesada y poco nemotécnica, será difícil de descubrir por los atacantes. Por ello, uno de los mayores problemas a efectos probatorios respecto a un acceso no autorizado radica en este punto; en los casos en que se fuerce a los usuarios a elegir contraseñas más complejas, es casi seguro que éstas se podrán encontrar anotadas en una pegatina en el cajón de su mesa de trabajo[15]. En este sentido, suele ser común que una persona que haya dispuesto de una información para fines ilegítimos, previo acceso autorizado a la misma, alegue que a pesar de que en el registro de accesos se haya evidenciado su usuario y contraseña en la fecha y hora del ultimo acceso, niegue el mismo sobre la base de que otra persona, bien desde su PC o bien utilizando sus claves de acceso al sistema electrónico, haya dispuesto de una información, suplantando su identidad, que con posterioridad su uso ha devenido en un tratamiento legitimo o ilegitimo. Sin embargo, pueden existir elementos comunes que

[13] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. *Protección de datos personales para Servicios Sanitarios Públicos*. Ed. Thomson.2008 – Civitas. p 80.

[14] Art. 93.1.- Real Decreto 1720/2007: *"El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios"*.

[15] AGENCIA DE PROTECCIÓN DE DATOS DE LA COMUNIDAD DE MADRID. *Seguridad y Protección de Datos Personales.* Ed. Thomson – Civitas.2009. pp 115 - 116

habiliten la confección de una prueba indiciaria suficiente para acreditar la autoría del acceso efectuado (tipo de información accedida, especialidad médica, uso ilegitimo realizado, comunicaciones realizadas, fechas y ubicación del acceso… etc.), destacándose igualmente que, cuanto mayor y más adecuado a la normativa vigente sea el sistema informático del centro sanitario, mayor rigurosidad adquirirán los datos que consten sobre un acceso ilegitimo. [16]

En cualquier caso, insistimos, en múltiples ocasiones, salvo cuando el documento ha sido suscrito mediante firma electrónica[17], nos encontramos ante la regla de las presunciones. Hipótesis que radican en acreditar una autoría determinada cuando por ejemplo un personal sanitario niega la admisión de un determinado acceso, o bien cuando cuestiona el propio contenido de un documento clínico cedido o extraviado (dicho contenido pudo haber sido alterado entre el envío y recepción de la orden de modificación).

Evidentemente, el problema de la autoría no se resuelve únicamente con el registro de un nombre de usuario y de una contraseña en el momento de encender el ordenador, pues resulta común en la práctica de los Centros dejarlo encendido mientras el empleado no está, o comunicar la clave de usuario o contraseña a otros compañeros de la Unidad o Servicio[18].

Por ello, si bien apuntábamos anteriormente que el deber de secreto se trataba de una obligación que debían de conocer todos los profesionales del centro sanitario, la elaboración de protocolos o códigos de buenas prácticas en la utilización y disposición de los recursos informáticos y no informáticos, constituye una conducta diligente por parte de la dirección del Centro que, en determinados

---

[16] STAP de Madrid, Secc. 16ª, 30 de junio de 2003 (JUR 2003\248747):
"Además, entendemos que, a la vista del contenido de los tres mensajes, la coincidencia de determinados contenidos, la proximidad de las fechas entre los 3 correos electrónicos, los días 2 de octubre y 29 de octubre de 2001 y 1 de noviembre de 2001, así como la utilización del mismo nombre del remitente " Claudio < DIRECCION000 ", entendemos con la parte recurrente que existen unos mínimos indicios para considerar que, al igual que el correo electrónico de 1 de noviembre de 2001 se atribuye indiciariamente a don xxxxxxx, en base a estos datos fácticos, también existen indicios suficientes para atribuirle al mismo imputado don xxxxxxx los correos electrónicos de fecha 2 de octubre de 2001 y 29 de octubre de 2001."

[17] Art. 3**.-** Ley 59/2003, de 19 de diciembre, de firma electrónica:
1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante
(…)
4. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel

[18] MÉJICA GARCIA, JUAN M. *La Historia Clinica: Estatuto Básico y Propuesta de Regulación*. Ed. Edisofer. Madrid. 2002. P.21

momentos, puede constituir un indicio adicional para la acreditación de una intromisión ilegitima en sus sistemas de tratamiento de información. Supone la prefijación de una serie de normas de conducta en el desempeño de las funciones profesionales que impliquen a su vez, por ejemplo, la obligación de mantener secretas las contraseñas o prohibición de comunicar contraseñas por teléfono o por correo electrónico.

2.1.2. El Documento de Seguridad

Tanto nos encontremos ante historias clínicas gestionadas en soporte papel como en soporte informático, se exigirá igualmente, al margen de dichos protocolos o códigos de conducta, la conformación de un Documento de Seguridad por parte del centro sanitario. Este Documento de Seguridad constituye un manual donde se recogerán las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.[19]

Como hemos expuesto, dentro de este Documento, uno de los principales apartados a desarrollar lo constituye el sistema de registro de accesos a la documentación protegida. Asimismo, la información sobre la identidad de todas aquellas empresas terceras que concurren en el acceso a la información clínica protegida con fines de prestación de servicios constituye otro de los elementos centrales de prueba para acreditar eventuales intromisiones o cesiones ilegitimas de información. Estos prestadores de servicios, dentro de su función, tienen prohibido destinar la información facilitada o accedida a finalidades distintas de las que motivaron su contratación; finalidad/es recogida/s en las estipulaciones del contrato suscrito con el centro sanitario en cuestión. En caso de una actuación contraria, bien a lo dispuesto en el clausulado del referido contrato bien a las instrucciones expresas del Centro responsable de la información, conforme al RD 1720/2007, motivará que se les considere, también, responsables del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Nos encontramos ante un Documento de obligada confección por parte del centro sanitario, como deudor de seguridad en materia de datos, debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, los datos de carácter personal puedan llegar a manos de terceras personas[20]. El propio Documento de

[19] Art. 88.- Real Decreto 1720/2007

[20] STAN, Sala de lo Contencioso Administrativo, Secc.1ª, 12 de noviembre de 2008 (JUR 2008\380816): *"Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas de seguridad para evitar que los datos se pierdan, extravíen o acaben en manos*

Seguridad constituye una prueba esencial para determinar, sobre la base de las medidas de índole técnica y organizativa que se describan, qué elementos de prueba solicitar al Centro, a través de la autoridad competente, para intentar acreditar un tratamiento ilegitimo de información clínica personal. Dicha idoneidad viene determinada por el contenido mínimo que debe de reunir el mismo para el tratamiento de datos personales relativos a la salud de las personas[21]. De nada sirve que se aprueben unas instrucciones de índole técnica y organizativa para el tratamiento seguro de la información clínica si, en la realidad del día a día del Centro, no se exige a los empleados su cumplimiento[22].

3. Incumplimientos y prueba

Conforme se ha expuesto en apartados anteriores, en el funcionamiento de una institución sanitaria confluyen numerosos agentes autorizados (personal sanitario y no sanitario) en el acceso y tratamiento de la información clínica custodiada. Todos y cada uno de estos profesionales tienen encomendadas distintas funciones que, conforme a la normativa vigente, deben de determinar tanto el tipo como el alcance de sus accesos[23].

Esta disparidad de funciones y accesos provoca que en las instituciones en donde no exista una política de información y control de los mismos, generalmente por un desconocimiento de las obligaciones legales que la normativa impone en este aspecto, la concurrencia de situaciones por todos conocidas, como abandono de historias clínicas en lugares públicos (basura municipal), accesos por parte de terceros a historias clínicas por medios telemáticos (Internet) o cesión de datos de salud para su difusión publica a través, por ejemplo, de un tercero. Dentro de la enorme casuística y pronunciamientos judiciales sobre accesos, tratamientos y cesiones ilegítimas de información sanitaria que podemos encontrar en los archivos, conviene enumerar tres de los principales ámbitos y/o prácticas de intromisión.

3.1. Ámbito Laboral

---

de terceros. En definitiva todo responsable de un fichero(o encargado de tratamiento), es, por disposición legal, deudora de seguridad en materia de datos, debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica sin que, bajo ningún concepto, datos bancarios o cualesquiera otros datos de carácter personal puedan llegar a manos de terceras personas."

[21] Art.88.- Real Decreto 1720/2007

[22] STAN, Sala de lo Contencioso Administrativo, Secc.1ª, 12 de noviembre de 2008 ((JUR 2008\380816): *"No basta con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Así, de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder para la recogida y destrucción de documentos que contengan datos personales si luego no se exige a los empleados (...) la observancia de aquellas instrucciones."*

[23] Art. 89.- Real Decreto 1720/2007: "*Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad".*

Por regla general, uno de los aspectos más controvertidos en el presente ámbito lo constituyen las revelaciones de datos sanitarios obtenidos con ocasión de los distintos controles médicos realizados en el ámbito de la "vigilancia de la salud" regulado por la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL). En efecto, este tipo de controles suelen ser el caldo de cultivo de numerosos despidos laborales[24].

En diversas ocasiones, en los despidos por ineptitud sobrevenida, suelen apreciarse indicios probatorios de filtraciones de información sensible del trabajador a la que única y exclusivamente puede tener acceso el personal medico interviniente y no el empresario; este último, salvo consentimiento expreso del trabajador, únicamente puede ser informado de las conclusiones del reconocimiento médico en términos de Apto o no Apto, pero nunca, de las motivaciones clínicas que provoquen una declaración de ineptitud.

Un caso de filtración podemos encontrarlo en aquellas cartas de despido en las que se pone de manifiesto un cuadro clínico o patología concreta del trabajador como causa del cese laboral (Ej: *Las razones que han llevado a la empresa a tomar esta decisión son fundamentalmente el haber tenido conocimiento de su ineptitud sobrevenida para continuar prestando los servicios (…) situación incompatible con la dismetría que presenta en los miembros inferiores y le causa problemas de espalda* (…)" y máxime cuando, en relación al ejemplo trascrito, se trataba de una patología como era una dismetría permanente de uno de los miembros inferiores del trabajador, no puesta de manifiesto como causa de ineptitud sobrevenida en controles médicos anteriores al que motivó el cese laboral[25].

En este caso, uno de los medios de prueba necesarios al objeto de acreditar o desacreditar una filtración ilegitima como la descrita, lo constituye la aportación del consentimiento del propio afectado (trabajador) por parte del empresario. En relación con este consentimiento, la Audiencia Nacional señala, que el mismo debe ser expreso, no admitiéndose por tanto ni el consentimiento tácito ni presunto. Por consentimiento expreso hemos de entender aquél que se obtiene de una declaración clara e inequívoca por parte del interesado que acepta o rechaza la cesión y uso de sus datos mediante la expresión de su voluntad, de forma que permita su constancia y prueba indubitada. La

[24] Art. 22**.-** Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales
"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."*

[25] STAN, Sala de lo Contencioso Administrativo, Secc. 1ª, 9 de junio de 2009 (JUR 2009\363726)

existencia de consentimiento expreso, referido a la cesión y uso de estos datos especialmente sensibles, no debe admitir duda, ni entenderse o interpretarse en varios sentidos, o poder dar ocasión a juicios diversos. Así, el responsable de la información debe de contar con los medios de prueba necesarios que acrediten dicho consentimiento expreso toda vez que el afectado, no debe de aportar nada más que su negación expresa a que hubiera prestado tal consentimiento[26]. La finalidad perseguida por la LPRL, consistente, precisamente, en establecer un eficaz sistema preventivo de dichos riesgos, descansa sobre la disposición de los trabajadores a someterse a controles preventivos, lo que sería difícil de lograr sin asegurar la absoluta confidencialidad de la información obtenida.

Dentro del ámbito analizado, podemos encontrar casos de cesiones ilegitimas de información clínica de un mismo trabajador por parte de las Mutuas de Prevención de Riesgos Laborales (Mutua/s) a distintas empresas. En el caso analizado, la cuestión se centra en examinar la legitimidad de una cesión de datos de salud por parte de una Mutua a una empresa, que había obtenido de un examen médico realizado a un trabajador cuando el mismo estaba al servicio de otra empresa de la cual, la Mutua era la misma. La consecuencia fue el despido del trabajador por su nueva empresa. Así, el debate se centra en analizar si en esta cesión concurre la habilitación legal dispuesta en el art. 11.2 de la LOPD[27]. La Audiencia Nacional, Sala de lo Contencioso Administrativo, estimó la no concurrencia de infracción mediante sentencia de fecha 24 de mayo de 2005, sobre la base de que la expresión "conclusiones" del art. 22.4 de la LPRL, no ha ser interpretada de manera restrictiva; existe un principio de unidad de historia clínica, justificado por la necesidad de una gestión eficaz de la asistencia sanitaria.

Sin embargo, posteriormente, el Tribunal Supremo, en la resolución del recurso de casación planteado por el afectado, lejos de compartir tal argumentación, destacó que las historias clínicas no deben tener carácter unitario para facilitar su misión a las mutuas de prevención de riesgos laborales y menos aún a los empresarios. En esta materia, concluye la Sala, que rige incuestionablemente la máxima confidencialidad posible, sin que haya elemento alguno en la LPRL o en la LAP que permita afirmar que la comunicación de datos no consentida llevada a cabo por la Mutua estaba autorizada por una ley[28].

---

[26] STAN, Sala de lo Contencioso Administrativo, Secc. 1ª, 9 de junio de 2009 (JUR 2009\363726)

[27] Art.11.2.- LOPD: "*El consentimiento exigido en el apartado anterior no será preciso: A) Cuando la cesión está autorizada en una ley".*

[28] STS, Sala de lo Contencioso Administrativo, Secc. 6ª), 20 de octubre de 2009 (RJ 2009\7551): "*(…) las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo" constituye una excepción. Y las excepciones, como es bien sabido, han de ser interpretadas restrictivamente. En este supuesto, además, ello resulta reforzado por una consideración teleológica innegable: si lo que debe protegerse ante todo es la confidencialidad de la información sanitaria relativa a los trabajadores, no tiene sentido afirmar que cabe comunicar a los empresarios cualquier dato que exceda de la mera "conclusión" sobre la idoneidad del*

Por tanto, la figura de la acreditación por parte de la Mutua de haber recabado el consentimiento expreso del afectado para la cesión de su información clínica se reviste nuevamente como el elemento central de este tipo de procedimientos con un trasfondo laboral, si bien, en estos casos, la simple negación de haber consentido por parte del afectado, implica la carga de probar lo contrario por parte del responsable de la información, al objeto de evitar la sanción pertinente.

3.2. Prospección Comercial

La Sociedad de la Información en la que vivimos actualmente, facilita sobremanera la trasferencia indiscriminada de todo tipo de información comercial entre los ciudadanos.

Detrás de este tipo de envíos masivos de publicidad se esconden, en un gran número de casos, intromisiones ilegítimas en la intimidad de las personas así como cesiones no autorizadas de información sensible. Son comunes los casos en los que un paciente, intervenido quirúrgicamente de una dolencia o tratado medicamente de algún tipo de patología, recibe propaganda comercial de diferentes entidades especializadas en productos para el tratamiento de su problema de salud. Obviamente, a salvo de que se haya dado un consentimiento expreso por parte del paciente en cuestión, tales acciones de prospección comercial provienen, en la gran mayoría de las ocasiones, de cesiones ilegitimas, o filtraciones de seguridad, de información por parte del centro sanitario para su posterior uso en finalidades distintas a la puramente asistencial.

Un claro ejemplo de estas prácticas ilegitimas, que en ocasiones albergan trascendencia penal, lo podemos encontrar en el caso de un profesional médico que ordenaba a su secretaria la obtención de las identidades de las pacientes sometidas a un proceso quirúrgico (histerectomías con doble anexectomía – extirpación de útero y ovarios), mediante el acceso a los archivos de anatomía patológica, a fin de enviar a las mismas propaganda de su clínica privada, y de los tratamientos que allí se realizaban[29].

En estos casos, bien tratándose de un sistema de gestión electrónica, bien tratándose de un sistema de gestión manual, un elemento de prueba necesario lo constituye el registro de accesos a los distintos historiales clínicos de los pacientes. En los mismos, debe de registrarse específicamente 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, así como que en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

---

trabajador para el puesto de trabajo; es decir, la mutua sólo puede decir al empresario si reputa apto al trabajador, sin proporcionarle ninguna otra información adicional."

[29] STS, Sala de lo Penal, 4 de diciembre de 2001 (RJ 2002\817)

Sin embargo, en el caso expuesto, a pesar de que el acceso realizado se ha llevado a cabo por un profesional sanitario, la finalidad del tratamiento realizado, prospección comercial, es claramente incompatible con la finalidad que motivó el consentimiento de las pacientes, sin que pueda encuadrarse una práctica como la descrita, en ninguno de los supuestos excepcionales contemplados por el RD 1720/2007[30]; excepciones a la obtención del consentimiento expreso e inequívoco de los/las afectados/as que se centran en usos posteriores con fines históricos, estadísticos o científicos.

4. Conclusiones

Si bien es cierto que en el día a día de los centros sanitarios y/o entidades que albergan en sus archivos información de salud de las personas, el tratamiento de la misma obedece a fines legítimos para el bienestar de los pacientes y/o ciudadanos, no es menos cierto que tales fines no pueden justificar en modo alguno un trato discrecional y arbitrario de dicha información sin contemplar las imposición legales que para dichos tratamientos la distinta normativa impone.

Estas obligaciones de seguridad y de respeto al principio dispositivo de la información personal de cada ciudadano, deben estar presentes en cada tratamiento que cada centro o entidad lleve a efecto para el cumplimiento de sus objetivos institucionales. Su inobservancia, al margen de constituir como se ha expuesto distintas infracciones legales, pueden conllevar importantes perjuicios para los afectados (laborales o personales).

Lejos de que la acreditación documental de una serie de medidas de seguridad constituya un eximente de la responsabilidad imputada, las infracciones en este materia, son también infracciones de resultado, esto es, es necesario que las mismas hayan producido la efectividad pretendida al objeto de evitar, no sólo las sanciones a las que puedan enfrentarse las instituciones, sino el perjuicio personal sufrido por los afectados; estos, a pesar de no ser profundos conocedores de los complejos sistemas de tratamiento de información o de los distintos tratamientos que de su información se lleven a efecto, ven reducido su esfuerzo probatorio, toda vez que la normativa en materia de protección de datos impone a los responsables de dicha información la prueba de la existencia, entre otros, del consentimiento del afectado para el tratamiento concreto de datos que se haya denunciado.

[30] Art. 9 .- Real Decreto 1720/2007: *"No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos. Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.*