

CONFIDENCIALIDAD Y SECRETO MÉDICO



Ilustre Colegio Oficial de Médicos
de la Provincia de Badajoz

CONFIDENCIALIDAD Y SECRETO MÉDICO



Coordinadores

Pedro Hidalgo Fernández
Carlos López Bernáldez
Mariano Casado Blanco

Autores

Mariano Casado Blanco
Manuel Fernández Chavero
Ceciliano Franco Rubio
Juan Calixto Galán Cáceres
Carlos López Bernáldez
Julio López Ordiales
Paloma Moyano López
Jorge Mariño Del Real
Félix Suárez González

Edita

FUNCOMBEA
*(Fundación Ilustre Colegio Oficial de Médicos
de la provincia de Badajoz)*

Imprime

Efezeta, Artes Gráficas, S.L.

Depósito legal

BA-482-2016

ISBN

978-84-617-4968-3

Queda prohibida, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra sin contar con la autorización de los titulares de su propiedad intelectual.

ÍNDICE

PRÓLOGO

Dr. D. Pedro Hidalgo Fernández

Presidente del Ilustre Colegio Oficial de Médicos de la provincia de Badajoz

09

EL SECRETO PROFESIONAL MÉDICO Y LA PROTECCIÓN A TERCEROS

**El deber del secreto y la obligación de los médicos
y resto de profesionales sanitarios: aspectos jurídicos.**

Nueva regulación

Sr. D. Juan Calixto Galán Cáceres

Fiscal Jefe de la Fiscalía Provincial de Badajoz

17

**El secreto profesional:
concepto y regulación deontológica y jurídica**

Prof. Dr. D. Mariano Casado Blanco

Presidente de la CCPMEx

33

**Confidencialidad, la custodia de la Historia Clínica
en modelo tradicional y en la historia clínica informatizada**

Dr. D. Ceciliano Franco Rubio

Director Gerente del Servicio Extremeño de Salud

55

Seguridad de información clínica en las bases de datos

Sr. D. Julio López Ordiales

Fiscal Delegado Provincial de Criminalidad Informática.

Fiscalía Provincial de Badajoz

75

PROBLEMÁTICA DE LA CONFIDENCIALIDAD EN LOS DIFERENTES MEDIOS DE LA MEDICINA

En Atención Primaria

Dr. D. Félix Suárez González

Médico de Familia. Centro de Salud San Roque. (Badajoz)

93

En Medicina del trabajo

Dr. D. Manuel Fernández Chavero

Especialista en del Trabajo

103

En Investigación Clínica

Dña. Paloma Moyano López

Coordinadora del CICAB

117

En Hospital

Dr. D. Jorge Mariño Del Real

Jefe del Servicio de Urología. HIC. (Badajoz)

129

En Formación

Dr. D. Carlos López Bernáldez

Profesor Asociado en Ciencias de la Salud.

Facultad de Medicina UEx. (Badajoz)

137

*"A todos los que a diario escuchan, guardan
y atienden a personas enfermas"*

Junta Directiva del icomBA

PRÓLOGO

Pedro Hidalgo Fernández

*Presidente del Ilustre Colegio Oficial de Médicos
de la provincia de Badajoz*

La esencia de nuestra profesión se basa en la CONFIANZA.

Confianza entre dos personas, una que sufre y una que quiere ayudar. Una que habla, se sincera y explica, y la otra que escucha, anota y guarda todo lo que su paciente le confiesa y de lo que él le hace depositario y custodio.

Tenemos asumido, desde el inicio de este oficio – arte y profesión - que cuando la puerta de la consulta o de la habitación se cierra, con ella se sella la boca del médico que interroga y oye al paciente. Sin llegar a firmar documento o contrato previo. Se sabe. Se da por sabido y no se cuestiona, pues no se entendería que fuese de otra manera.

Sabemos, médicos y pacientes, que el profesionalismo en la práctica de la medicina precisa de un VÍNCULO DE CONFIANZA.

El buen quehacer del médico necesita de unos pilares de discreción, sigilo, custodia y secreto.

Desde el inicio así se entendió y fue Maimónedes o Hipócrates (460 a.c.) el que lo plasma en su Juramento como “callaré todo lo que en el ejercicio de la profesión y hasta fuera de ella pueda ver y oír”. Y en eso no se ha cambiado, por estar asumido por médico y paciente. Pero la modificación viene cuando el deber del médico llega a tener consideración de derecho del paciente, con un cambio de modelo que lleva del paternalismo a la autonomía. Del tú me informas que yo decido. Del te digo, te pregunto y decido.

Los secretos derivan de que los hombres guardan reservada una parte de su yo, guardan una intimidad que les aísla, les diferencia, les hace individuos frente a los demás hombres con los cuales conviven¹. Porque a fin de cuentas la “intimidad constituye uno de los bienes fundamentales de la persona humana”².

Tiene el Código de Deontología Médica todo el Capítulo V dedicado al Secreto Profesional del Médico y en seis artículos y dieciocho apartados desarrolla las reglas de actuación para autorizarnos como garantes de todo lo revelado y deducido del estudio de un paciente y de su Historia Clínica y estableciendo “*por el hecho de ser médico no se te autoriza a conocer información confidencial de un paciente con el que no tenga relación profesional*” (art. 27.3).

¹ J.A. MARTÍ MERCADELL. *Ética y medicina*. Ed. Espasa Calpe S.A. Madrid. 1988, pág. 84.

² ANTONIO DE LORENZO. *Deontología y Medicina*. Colegio Oficial de Médicos de Madrid, 1977, pág. 491.

Las palabras claves de nuestro secreto serían: confianza, intimidad, privacidad, ética, paciente, profesión, derechos y leyes. Pero la sustancia es que un hombre (enfermo) busca a otro hombre (médico) para que le ayude.

La existencia del secreto profesional, y concretamente del Secreto Médico, deriva de la existencia de la intimidad y del hecho de que el hombre es un ser social. La necesidad nacida del instinto natural de conservación. El secreto médico no es solo el respeto de un derecho, el derecho del hombre – paciente a la intimidad, sino también un beneficio social. Es la sociedad la que sale beneficiada de la existencia del secreto médico³.

El secreto médico es en algunos aspectos muy superior al de confesión, dado que el penitente muchas veces permanece anónimo y que el sacerdote ha de hacer un esfuerzo para olvidar una vez dada la absolución. El paciente, en cambio, no es un anónimo, que se ve obligado por necesidad a decir toda la verdad y quizás cosas de los demás, de sus antecesores y, además, el médico no debe procurar olvidarlo, sino al contrario, tomar nota escrita de ello para no hacerlo⁴.

Todo este pensamiento nos llevó a organizar en nuestro Colegio de Médicos de Badajoz, el quince de junio de este año, una jornada con el título CONFIDENCIALIDAD Y DERECHO MÉDICO, dónde abordaban, en el primer módulo EL SECRETO PROFESIONAL DEL MÉDICO Y LA PROTECCIÓN A TERCEROS, expresando el deber de secreto que tiene el médico y el derecho a la confidencialidad que tiene el paciente, así como las garantías de archivo y custodia que deben reunir la información clínica obtenida y recogida en la Historia Clínica. El segundo módulo trató de la PROBLEMÁTICA DE LA CONFIDENCIALIDAD en el medio hospitalario, en la medicina del trabajo, en la atención primaria y en la investigación sanitaria. Agradezco a los autores D. Carlos López Bernáldez, D. Juan Calixto Galán Cáceres, D. Mariano Casado Blanco, D. Ceciliano Franco Rubio, D. Julio López Ordiales, D. Félix Suárez González, D. Manuel Fernández Chavero, Dña. Paloma Moyano López y D. Jorge Mariño del Real, el esfuerzo de síntesis y de actualización que han hecho en sus diferentes apartados.

Tenemos que valorar la confianza social en la reserva de la profesión médica. Si no existiera el compromiso de los médicos de salvaguardar la confidencialidad, los pacientes no se acercarían a la consulta confiadamente. La falta de información deri-

³ J.A. MARTÍ MERCADELL. *Ética y medicina*. Ed. Espasa Calpe S.A. Madrid. 1988, pág. 87, 88 y 89.

⁴ LAWRENCE R. BURNS. *Journal of clinical computing*, Vol. 4, nº 1, 1974, pág. 21. 166, Morris Av. N.Y.

vada de esta desconfianza podría llegar a perjudicarles seriamente. Las consecuencias de una medicina sin confidencialidad serían muy graves para la sociedad. Se trata pues de una justificación utilitarista del deber de secreto⁵.

Vemos como la confianza del paciente y la confidencialidad del médico ayudan a la sociedad y a la persona. Busca unir deber y obligación en un pacto que se da sobreentendido.

El derecho a la intimidad deriva de los derechos fundamentales a la vida, libertad y propiedad. La intimidad constituye un derecho de la personalidad y como tal ha de ser considerado como irrenunciable, inalienable e imprescindible. Los datos médicos forman parte de la esfera más íntima de la persona⁶.

No hemos hablado de las enfermedades, hemos hablado de personas que tratan de curarse o auxiliarse a través de la medicina que ejerce otra persona, y que debe de ofrecerle no sólo lo mejor de su ciencia sino además el mejor de sus silencios, sea cual fuere el método donde lo guarde o archive.

Debemos asumir que la protección al derecho a la intimidad esté entre los indicadores de calidad⁷.

Desearíamos desde la Corporación Colegial, que este libro sea de lectura fácil e interesante, pero de plena aplicación en el día a día del ejercicio de nuestra profesión.

⁵ MARIA TERESA DELGADO MARROQUÍN, *med. 06 (Confidencialidad y Secreto Profesional)* pág. 13. Tit. Experto en Ética Médica, OMC 2015.

⁶ CARMEN SANCHEZ CARAZO, *La intimidad y el Secreto Profesional*; Ed. Díaz – Santos. 2000.

⁷ M.J. SERRANO GONZÁLEZ, *La importancia del secreto médi*

EL SECRETO PROFESIONAL MÉDICO Y LA PROTECCIÓN A TERCEROS

**EL DEBER DEL SECRETO
Y LA OBLIGACIÓN DE LOS MÉDICOS
Y RESTO DE PROFESIONALES SANITARIOS:
ASPECTOS JURÍDICOS.
NUEVA REGULACIÓN**

Juan Calixto Galán Cáceres
Fiscal Jefe de la Fiscalía Provincial de Badajoz

Podemos afirmar que el derecho al secreto de los datos personales es un atributo de la personalidad cuya protección emana del derecho a la intimidad personal y familiar de las personas, incluso de su propia imagen, del modo que sanciona nuestro texto constitucional en el art. 18 otorgándole en su calidad de derecho fundamental de las personas la mayor protección y el máximo calado jurídico.

Hasta tal punto es consciente el legislador constitucional que en el art.18.4 CE expresa que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”* en una interpretación que acoge el T.C. (S. 254/93 de 20 de julio) y que a su vez se hace eco de dos aspectos consagrados en la jurisprudencia constitucional (TC Alemán S^a 15/83):

De esta consideración de sustancial importancia emana su dimensión jurídico penal en la medida en que como bien jurídico protegido digno de tutela el Legislador decide elevar a rango delictivo determinadas conductas que vulneran esa protección constitucional de la intimidad personal y por ende del derecho al secreto por parte de su titular del ámbito de su privacidad y de aquellos datos personales e intransferibles que no desea o no deben ser conocidos por terceras personas.

Estas afirmaciones en su vertiente constitucional han sido notablemente consolidadas por el propio Tribunal Constitucional (TC), quien en diversas resoluciones (SSTC 73/1982-EDJ1982/73- y 57/1994-EDJ1994/1755- entre otras muchas) ha incidido en que La idea de secreto en el art. 197,1^o C. penal resulta conceptualmente indisociable de la de intimidad: ese *“ámbito propio y reservado frente a la acción y el conocimiento de los demás”*.

Por ello en el Código Penal dentro del Título X de su Libro 2^o y en su Capítulo I se regulan los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y en el ámbito de esta protección penal de la privacidad personal se detallan hasta 7 tipos penales que inciden en diversas maneras y circunstancias donde se procede a la vulneración de ese derecho personal e intransferible que representa la intimidad y la confidencialidad de los datos personales.

Como el objeto de esta aportación se centra en la protección del secreto médico y en una reseña jurisprudencial que nos ayude a comprender cuándo determinados comportamientos del personal sanitario son elevados a la categoría de delito y sancionados por los Juzgados y Tribunales, por razones de oportunidad y de extensión, no recalaremos en todas las figuras penales, sino solamente aquellas que de modo especial nos interesan y son más genuinas en el ámbito del propio secreto médico, significando que los datos concernientes a la salud de las personas están dotado de

un plus de protección en la medida en que son datos sensible o como algunos autores denominan “*datos que pertenecen al núcleo duro de la intimidad*”.

Así debemos recordar que el primero de los preceptos en su art 197 señala:

- 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*
- 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.*

De estas modalidades es preciso significar tres importantes acotaciones, la primera es que no cabe una imputación a título de culpa o imprudencia, ya que las figuras tienen una estructura claramente dolosa o intencionada, la segunda es que la brevedad y puntualidad en el acceso por parte del autor, así como la valoración de tiempo, lugar y circunstancias van a influir en la decisión de los Tribunales como luego veremos, y en tercer lugar y finalmente tal y como se recoge en la STS de 30 de diciembre de 2009 “*los delitos recogidos en el 2º apartado del artículo 197, tienen un sentido claramente distinto a los recogidos en el apartado 1º: ya que las conductas afectan a datos que no están en la esfera de custodia del titular, sino en bancos de datos y pueden causar perjuicios a terceros distintos del propio sujeto al que se refiere la información concernida.*”

En los párrafos siguientes de este precepto se contienen agravaciones de la pena y calificaciones cuando hay difusión o cesión de los datos, cuando no se ha participado de modo directo pero se sabe del origen ilícito del acceso y utiliza los datos conseguidos, se eleva la pena a los responsables de los ficheros y archivos, e igualmente – y ello si es que es relevante en materia de secreto médico- se expresa que las penas se impondrán en el grado superior cuando los datos personales objeto del delito afecten, entre otras circunstancias, a la salud de las personas y también mayor pena si la actividad se realiza con fines lucrativos.

Recientemente y con motivo de la LO de 30 de Marzo del 2.015 de reforma del C.P. se añadió un nuevo precepto que tiene incidencia en las vulneraciones del secreto médico, en concreto el art 197 bis cuyo párrafo 1 expresa

- 1.- *El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.*
2. *Del mismo modo y también introducido por la citada reforma se castiga al que no realiza personalmente las conductas delictivas pero facilita a tercero para que realice los delitos proporcionando un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.*

Las penas se elevan en el supuesto de organización criminal, y atención porque ello si es importante se contempla por primera vez en nuestra legislación penal que estos delitos que hemos mencionado de descubrimiento y revelación de secretos se puedan cometer por una persona jurídica responsable en cuyo caso la penas es de multa de 6 meses a 2 años, pero además con posibilidades de imposición judicial de medidas (entre otras) tan drásticas y terminantes como la disolución de la persona jurídica, la clausura de sus locales, la inhabilitación para recibir subvenciones y ayudas públicas o la intervención judicial de la organización de la persona jurídica.

Ello obliga inexcusablemente a una reflexión en cuanto a la posible afectación de este tipo penal a personas jurídico- públicas o de naturaleza mixta, como son los Colegios Profesionales, entre ellos los Colegios Oficiales de Médicos.

Ni que decir tiene que esta problemática ha levantado una amplia polvareda doctrinal y dentro de los propios colectivos profesionales, especialmente a partir de la visión interpretativa que proporciona la última Circular de la Fiscalía General del Estado 1 /2.016 donde literalmente se afirma corrigiendo el criterio sostenido en otra Circular del año 2.011” *Tras la inclusión de los partidos políticos y los sindicatos en el régimen de responsabilidad penal, debe rectificarse este criterio. Los Colegios profesionales no encajan en ninguna de las categorías mencionadas en el art. 31 quinquies, sin que quepa en este caso hacer una interpretación claramente extensiva de las personas jurídicas excluidas. Debe entenderse que el ejercicio de potestades públicas de soberanía o administrativas, por su tenor literal, resulta aplicable solo a las administraciones públicas y no a entes de naturaleza asociativa privada, como los*

Colegios profesionales, las Cámaras de comercio, los sindicatos o los propios partidos políticos”,

Estas consideraciones albergan de modo afirmativo la posibilidad de comisión delictiva por parte de los Colegios Profesionales al amparo de la nueva regulación del art. 31bis del C.P., especialmente en las omisiones e infracciones de los deberes de gestión, vigilancia, supervisión y control a fin de evitar las figuras delictivas, --entre las que de modo indudable se ubicarían las figuras reseñadas de descubrimiento y revelación de secretos -- y ello obliga a los Colegios Profesionales (incluido los de Médicos) al estar muy atentos y vigilantes en disciplinar unas medidas de seguridad eficaces y en la realización también, de una supervisión informática adecuada de sus Bases de Datos que contengan elementos personales y sensibles, así como en la elección del personal responsable y eficaz que asegure la confidencialidad y el buen uso de todos los datos de carácter personal que manejan estos Colegios Profesionales.

En el art 198 del C.P. se castiga también en el grado superior de la pena y con una inhabilitación que puede llegar a 12 años *a la autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaleciendo de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior.*

Este precepto tiene una significación importante, pues sitúa el plano de mayor reproche al culpable en el hecho de que por razón de las facultades de su cargo tiene la ventaja sobre los demás facultativos o personal sanitario de poseer mayor facilidad en el acceso a programas, historias clínicas o bases de datos a las que no tendría acceso, si no fuera precisamente por el cargo que le habilita para cometer el delito con mayor impunidad.

Aparte de estas figuras penales que hemos relatado y que inciden de manera directa en la vulneración del secreto médico, sin duda la de mayor calado o de carácter más genuino es la atinente al tipo del art 199 del C.P. cuando expresa:

- 1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.*
- 2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.*

Es evidente que el facultativo y el personal sanitario tienen un deber máximo de reserva y sigilo que insitadamente se traduce en el marco obligatorio de carácter profesional que se contiene en el Código de Deontología de la Profesión Médica, de Julio del año 2.011 en cuyo Capítulo V y art 27 se expresa:

1. *El secreto médico es uno de los pilares en los que se fundamenta la relación médico-paciente, basada en la mutua confianza, cualquiera que sea la modalidad de su ejercicio profesional.*
2. *El secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica.*
3. *El hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional.*
4. *En las instituciones sanitarias informatizadas los médicos directivos velarán por una clara separación entre la documentación clínica y la administrativa.*
5. *El médico no puede colaborar en ninguna base de datos sanitarios si no está garantizada la preservación de la confidencialidad de la información depositada en la misma.*
6. *El médico podrá cooperar en estudios epidemiológicos, económicos, de gestión, etc., con la condición expresa de que la información en ellos utilizada no permita identificar ni directa ni indirectamente, a ningún paciente.*
- 7.- *El médico preservará en su ámbito social, laboral y familiar, la confidencialidad de los pacientes.*

Ahora bien, todo lo que hasta aquí hemos mencionado, es objeto de una matización de suma importancia en el propio código penal, y es que en el art. 201 se significa:

Para proceder por los delitos previstos en este Capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

La referencia al término "persona con discapacidad necesitada de especial protección" ha sido introducida en sustitución de la anterior referencia al término "inca-paz", conforme establece el número 258 del artículo único de la L.O. 1/2015, de 30

de marzo, por la que se modifica la L.O. 10/1995, de 23 de noviembre, del Código Penal (B.O.E. 31 marzo). Vigencia: 1 julio 2015

- 1.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.
3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130.

Esta triple observación viene inducida sin duda por el carácter privado y de libre disposición que subyace en la legislación constitucional y ordinaria sobre el uso de los datos personales, lo que deja en manos del titular agredido el ejercicio de la acción penal, con la excepción de la prevalencia del cargo público, en cuyo caso la intromisión ilegítima en los datos privados tiene un reproche punitivo por la transgresión del correcto deber público del cargo, ajeno a otras consideraciones de carácter personal.

Realizadas todas estas consideraciones de orden técnico-legal, vamos a pasar al catálogo y comentario de una reseña jurisprudencial centrada en la vulneración del secreto por parte de los profesionales sanitarios, de modo especial cuando el sujeto activo del delito ha sido un médico facultativo.

En esta miscelánea jurisprudencial vamos a contemplar cómo y por diferentes motivos y modalidades se llevan a cabo accesos indebidos a las historias clínicas de los pacientes, y también entradas ilegítimas en los programas y bases de datos que contienen datos concernientes a la salud de las personas, y que son conocidos de modo subrepticio y ajeno a las correctas y encomendadas finalidades curativas o terapéuticas.

En primer lugar destacamos la (STS. Sala 2ª –4/Abril/2.001)

"El relato fáctico declara, en síntesis, que la acusada, médico residente en el Hospital dependiente de la Diputación Provincial de Valencia, fue requerida para prestar sus servicios profesionales, para prestar asistencia neurológica a una persona a la que reconoció por proceder ambas de una pequeña localidad. Al examinar su historial clínico advirtió, "como antecedente quirúrgico la existencia de dos interrupciones legales de embarazo, circunstancia ésta que fue manifestada a su madre la que, a la primera ocasión, en el pueblo, lo comunicó a la hermana (...)"

El motivo se estima. El hecho probado es subsumible en el art. 199.2 del Código Penal. Este delito protege la intimidad y la privacidad como manifestaciones del libre desarrollo de la personalidad y de la dignidad de las personas.

Se trata de un delito especial propio, con el elemento especial de autoría derivado de la exigencia de que el autor sea profesional, esto es, que realice una actividad con carácter público y jurídicamente reglamentada. La acción consiste en divulgar secretos de otra persona con incumplimiento de su obligación de sigilo, tal obligación viene impuesta por el ordenamiento, Ley General de Sanidad 14/1986, de 25 Abr., cuyo art. 10.3-EDL1986/10228- establece el derecho de los ciudadanos tienen derecho "a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias" y concurrente en el historial clínico-sanitario, en el que deben "quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica" (art. 6.1-EDL1986/10228-). En este sentido, la STC 37/1989-EDJ1989/1607-.

La acción típica consiste en divulgar los secretos de una persona entendida como la acción de comunicar por cualquier medio, sin que se requiera que se realice a una pluralidad de personas, toda vez que la lesión al bien jurídico intimidad se produce con independencia del número de personas que tenga el conocimiento. Por secreto ha de entenderse lo concerniente a la esfera de la intimidad, que es sólo conocido por su titular o por quien él determine. Para diferenciar la conducta típica de la mera indiscreción es necesario que lo comunicado afecte a la esfera de la intimidad que el titular quiere defender. Por ello se ha tratado de reducir el contenido del secreto a aquellos extremos afectantes a la intimidad que tengan cierta relevancia jurídica, relevancia que, sin duda, alcanza el hecho comunicado pues lesiona la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de vida humana (TC S 28 Feb. 1994-EDJ1994/1755-).

Igualmente es importante apreciar que la sentencia precisa entre otras consideraciones en otras consideraciones lo siguiente: *"La Sala no comparte el criterio que afirma la sentencia impugnada en el que refiere que la conducta de divulgar no tiene relevancia penal al no tratarse "más que de simples cotilleos propios de lo que en la actualidad se denomina prensa amarilla o del corazón". Y no se comparte porque la afirmación frivola sobre sentimientos de forma no ajustada a la realidad. La divulgación del hecho, en cuanto perteneciente a la intimidad, lesiona su derecho fundamental precisamente por quien está específicamente obligado a guardar secreto».-*

Si ya hemos hecho alusión a la normativa legal en cuanto al acceso de la HC, vamos a perfilar ahora, fundamentalmente de modo jurisprudencial algunos matices en relación con la *problemática de accesos indebidos a la HC*, los perfiles que estos problemas representan desde la legislación de protección de datos, y ciertamente de

modo especial analizando las consecuencias de las invasiones intolerables en el ámbito de la intimidad a través de un mal uso de la historia clínica y que determina para su autor la responsabilidad más grave en el ámbito del delito de revelación de secretos del artículo 197 de nuestro código penal.

En el reseñado ámbito penal, los comportamientos indebidos de acceso ilegítimo a la HC de una persona con finalidades torticeras y para uso propio en perjuicio del paciente se sancionan desde la perspectiva de la comisión de un delito de revelación de secretos como sucede en la Sentencia de Audiencia Provincial de Sevilla, Sec. 7ª, S 7-12-2011, nº 76/2011, Rec. 6122/2011, que básicamente se contrae a una condena a una Administrativa del Hospital Virgen Macarena de Sevilla que accede a la HC de su marido para luego alegarla en un Escrito de Defensa, donde ella era acusada de un delito de Malos Tratos familiares supuestamente inferidos a su marido y acusada por el art 153.2 del C.P. Recordemos previamente que nos dice el Código penal a propósito del delito de descubrimiento y revelación de secretos (que por cierto fue modificado por la LO de Junio del 2.010) .

La Sentencia es interesante por 2 cuestiones: La primera es que la Sala no condena a la administrativa que accede a la HC de su marido por el párrafo 5 (expresado anteriormente), y no le aplica esa cualificación ya que dice textualmente a estos efectos: *“es sabido que prevalerse supone el aprovechamiento de la función que se realiza para cometer un hecho delictivo con mayor facilidad, sin que se trate de una agravación especial anudada a la función pública, puesto que cualquier servidor público puede cometer cualquier clase de delitos en los que resulta irrelevante su conducción de ejercicio de función pública. De otra parte, aunque en el ejercicio de sus tareas como administrativa (desde marzo de 2006 secretaria de la Subdirección Médica de Calidad) en el hospital Virgen Macarena” de Sevilla, dependiente del Servicio Andaluz de Salud, podía solicitar al archivo listados de historias clínicas para revisión (ver folio 35 del procedimiento abreviado) por indicación de su superiores, no consta indubitadamente que lo hiciera en relación con la de autos. Por último, como se anunció y se explicitará más adelante, no hay constancia fehaciente de que para hacerse con la documentación accediese personalmente por otra vía al registro sanitario donde se custodiaba (archivos del hospital)”*.

Es decir, que no basta la mera condición de Administrativa de la responsable del delito para cualificar su conducta, sino que será necesaria una prueba concluyente del acceso de la misma, pero –ojo–, en sentido adverso, la Sala, en nuestra opinión de modo inteligente y acertado, valora el dato de que, aunque no se haya demostrado a ciencia cierta la autoría material del acceso al archivo de la HC, la mujer responde pues al margen de reafirmar el carácter reservado de los datos de la salud de

su marido, como de modo ilustrativo señala la sentencia “con independencia de que *no hay* en verdad una *prueba directa* de que la acusada se apoderó materialmente de los controvertidos documentos, es inferencia razonable que *de haber sido otra persona, actuó de consuno con ella, la única beneficiaria* de la obtención de los mismos visto el destino que se les dio, lo que de por sí supone ya por parte de la inculpada un uso ilegal y espurio del historial clínico de su ya ex-marido.

También en sentido condenatorio resulta interesante la Sentencia de la Audiencia Provincial de Valencia de 4 de Octubre del 2.011 Sec. 1ª, S 4-10-2011, nº 507/2011, Rec. 4/2011 en la que se condena a una enfermera que con ánimo de proteger a su hermana y a los hijos de ésta, accedió a la HC de la mujer pareja actual del ex-marido de su hermana y que presentaba importante problemas psiquiátricos con intentos de suicidio, y lógicamente le preocupaba la situación de sus sobrinos, cuando el padre ejercía el régimen de visitas acompañado de esa mujer, desvelando precisamente la problemática de salud de esa persona cuando su hermana intentaba modificar judicialmente a su favor el régimen de visitas. La Sala que también condena por el art. 197 utiliza el párrafo 3º que no enunciamos antes y que dice:

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Y además le aplica la agravación del párrafo 5º, que en la otra sentencia no hizo uso la Sala, ya que aquí si *estima que la enfermera se prevale de su condición pública como persona responsable de esos ficheros*. Lo que ocurre es que la Sala, sin estimar la Eximente de Estado de Necesidad que alegaba la Defensa, si le aplica a la responsable del delito como cualificada la Atenuante del art 21.7 en relación con el nº 3 del propio art 21, es decir la *atenuante analógica de estado pasional*, es decir que su inteligencia y voluntad estaban francamente afectada por la preocupación de la situación de su hermana y sus sobrinos ante la convivencia con una persona que había tenido problema psiquiátricos.

Muy interesante, pero con sentido absolutorio es la STS de 30 de Diciembre del 2.009 Sala 2ª nº 1328/2009, Rec. 1142/2009 que anula una grave sentencia condenatoria anterior de la AP de Baleares de 11 de Febrero del 2.009, por el que se había condenado a un médico por un delito continuado de acceso a la HC de un paciente también médico a la pena de 3 años y 3 meses de prisión, y 9 años de inhabilitación absoluta para empleo o cargo público, mediante un uso indebido del programa in-

formático, de manera que consiguió enterarse quien era el médico de cabecera del paciente.

Razona la Sala, a nuestro entender con buen criterio, que el hecho de que el acusado únicamente se haya enterado de ese dato (el nombre del médico que atendía al paciente), tiene para el hombre medio escasa relevancia jurídica, ya que en general es de fácil acceso y en muchos casos de público conocimiento, careciendo sin más de posible perjuicio para el paciente. No olvidemos en tal sentido, que al margen de discusiones doctrinales y jurisprudencial al caso, el bien jurídico protegido en el tipo penal, es la intimidad individual, y que el tipo penal del art. 197 exige al final de su nº 2 que la utilización o apoderamiento de algún dato debe ser en perjuicio del titular del dato o de un tercero. Y señala también que el apoderamiento y el acceso a la HC, deben conllevar un perjuicio en aquellos datos que no son sensibles como es este caso, en que el acceso era limitado al nombre del médico de cabecera, pero – ojo- si se trata de un dato sensible (que entendemos que en la HC son la mayoría de los mismos) , el TS deja claro que se castigaría como delito el mero acceso, pues el perjuicio al titular ciertamente ya lo infringe la persona que indebidamente accede a esos datos de la HC sin estar autorizada. Obviamente con mucho más motivo la utilización o modificación de cualquier dato de la HC.

Es preciso consignar, que en realidad en los accesos indebidos a la HC, el precepto que realmente entra en juego es el nº 2 del art. 197 (a menudo con la aplicación de los números 5 y 6 de ese precepto), y que precisamente el nº 2 como tipo básico expresa “datos reservados”. No olvidemos, que los tipos penales por imperativo legal son de interpretación estricta, y las palabras que definen un delito nunca tienen interpretación extensiva, por lo que “reservado” en gran medida gramaticalmente tiene un componente de sensibilidad, y de protección frente a lo que es público o de fácil conocimiento. Por ello la AP de Navarra en ST de 20 de Septiembre del 2.011, Rec. 12/11, en la misma línea que la sentencia anterior absuelve a un médico que accede en 2 ocasiones a la HC de una persona que no era paciente suya, y en tal sentido aunque la Sala reconoce que los accesos son indebidos, no se demuestra que tuviera conocimiento con esos acceso de datos reservados, sino que esos datos relativos a la salud de la persona de la HC y que pudo conocer con el acceso, en realidad ya los tenía en el expediente médico que manejaba del paciente respecto de una empresa sobre la que iba a formular una Pericial. En concreto se manejaban datos relativos al consumo de alcohol que al parecer, ya figuraban en el expediente médico del interesado al margen de su propia HC.

Ciertamente en mi opinión, esta segunda sentencia emitida por la AP de Navarra, es francamente discutible y en general no compartimos la argumentación de la

misma. Del contenido de la sentencia, si parece haber existido un acceso no autorizado e intolerable a la HC de una persona respecto de la que el médico no la tiene como paciente, y a diferencia de la anterior sentencia, donde sólo consiguió saber el nombre del médico, en esta sentencia si hay una intromisión de fondo en la intimidad personal del que se quiere conocer sus secretos, sólo con el matiz de que la HC era similar o contenía datos que estaban también en el expediente médico empresarial, pero por ello en nuestra opinión, se verifica claramente el acceso a datos reservados, aunque los mismos figuren en un expediente, que por razones concretas y particulares también conoce el médico, pero este dato- y con todas las reservas no disponer de toda la documentación, ni haber realizado el juicio oral- no decae la tipicidad de la conducta del acusado, ya que el acceso a datos reservados, Sí se produce, *ya que esos datos relativos a la salud personal del interesado siguen siendo reservados, sin que pierdan esa condición porque ocasional o eventualmente figuren en otro expediente ajeno a su HC.*

De modo que, con la lógica prudencia de no conocer en su integridad todas las actuaciones, respetuosamente, no compartimos en modo alguno la tesis absolutoria que formula la Audiencia, y la de nuestro compañero Fiscal que intervino en la causa, el cual no formuló Acusación por estos hechos, participando de la tesis absolutoria.

Fuera del art. 197, y en el ámbito de la divulgación o revelación de secretos mencionamos la S. Audiencia Provincial de Zaragoza, Sección 1ª, Sentencia de 27 Jul. 2011, Rec. 157/2011, donde es condenada una persona que trabajaba de Técnico de laboratorio y comenta pública e indebidamente que una persona había dado positivo al virus VIH, y la noticia llega al interesado antes de los cauces oficiales. Se le impone 1 año de prisión y 6 meses de multa, fijando una indemnización a favor del perjudicado en 6.000 euros.

Con carácter muy reciente es destacable la Sentencia del Tribunal Supremo Sala 2ª, S 3-2-2016, nº 40/2016, rec. 943/2015 en cuyos hechos probados se relata que: Esteban, funcionario de la Comunidad Autónoma de Illes Balears (CAIB) en cuanto médico de Salud Pública del Centro Insular de Sanidad de Menorca, sin antecedentes penales, y Paula, también funcionaria de la CAIB en cuanto enfermera del mismo Centro, mantuvieron una relación sentimental de duración indeterminada, la cual a finales del año dos mil nueve había ya finalizado.

Desde ese momento, la relación entre ambos quedó muy deteriorada, hasta el punto en que, pasado el tiempo, y tras varios episodios de desencuentros laborales y personales, el día veintiocho de Septiembre de dos mil diez, el Sr. Esteban, tras haber cruzado varios mensajes de texto a través de teléfono móvil con la Sra. Paula, remitió

a ésta uno en el que, al hilo de su discurso, le llamaba "PUTA ambmayuscules" y "merda pura".

Una vez conocida esta tensa situación por la Administración de la Comunidad Autónoma de Illes Balears, año dos mil once, se incoó Expediente Disciplinario, referenciado con el N° NUM000, frente al Sr. Esteban, consecuencia del cual la Sra. Paula tuvo conocimiento de los accesos informáticos no consentidos que a su historial clínico y al de sus familiares habían tenido lugar por parte del Sr. Esteban, sufriendo una crisis de ansiedad y causando por tal motivo baja laboral el día veintisiete de Abril de dos mil once, prolongándose la misma hasta el día treinta y uno de Octubre siguiente, comportando a la CAIB un total de 2.358,17 euros en concepto de prestaciones laborales.

En efecto, desde el día uno de Diciembre de dos mil nueve hasta el día nueve de Febrero de dos mil once, Esteban, sin consentimiento ni conocimiento de Paula, ni de ningún familiar de ésta, amparado en su condición de funcionario médico de la CAIB, lo cual le permitía acceder a los sistemas de información del IB-Salut, y siendo consciente del compromiso de confidencialidad que había contraído en fecha dieciocho de Noviembre de dos mil nueve, efectuó un total de ciento setenta y un accesos a las historias clínicas (ESIAP, o Sistema de Información de Atención Primaria) de aquella y su familia; en concreto, setenta y seis a la de Paula; cincuenta y un accesos a la de quien era su esposo, Baltasar; treinta y seis a la de la hija de ambos, Sagrario; y ocho a la de la hermana del Sr. Baltasar, Salome.

Igualmente, durante el mismo periodo de tiempo y en iguales circunstancias a las anteriormente citadas, el Sr. Esteban accedió veinte veces a la Historias de Salud (HSAL) de Paula, veintinueve veces a la de Baltasar, doce a la de Sagrario y una a la de Salome”

Al médico se le condena a una pena de 3 años y 3 meses de prisión, multa de 20 meses y suspensión de empleo público de funcionario del ICAIB por tiempo de 2 años.

En torno a la lesión psíquica sufrida por la víctima dice el Tribunal: Ciertamente, el perjuicio al que se refiere el tipo penal no es la lesión psicósomática declarada concurrente, ésta es una consecuencia de la conducta que deberá ser tenida en cuenta para fundar, como hace la sentencia, la responsabilidad civil. (Se le otorga a la misma una indemnización de 6.000 euros a pagar por el penado).

La sentencia del máximo tribunal ordinario efectúa 2 importantes apreciaciones:

- 1.- Caracteriza, por lo tanto, esta figura típica tratarse de datos propios de la intimidad de una persona guardadas en bases de datos no controladas por el ti-

tular del derecho, y, por ende, sujeta a especiales normas de protección y de acceso que el autor quiebra para acceder. El carácter sensible de los datos a los que se accede incorpora el perjuicio típico.

- 2.- Como dice la STS 532/2015, de 23 de septiembre, en principio todos los datos personales analizados son "sensibles" porque la ley no distingue a la hora de darles protección y el tipo penal prevé una agravación (art. 197.6 CP) para los supuestos en los que el objeto sea especialmente sensible, afectando a ideología, religión, creencias, origen racial o vida sexual.

El perjuicio se realiza cuando se apodera, utiliza, modifica o accede a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos, archivo, etc, especialmente protegido, porque no es custodiado por su titular sino por titulares de las bases con especiales exigencias de conductas de protección.

Es muy interesante la STS del Tribunal Supremo de 22-10-2013, nº 778/2013, rec. 1949/2012 que rectifica y anula la Sentencia de la Secc. 1ª de la Audiencia Provincial de Valencia de 30-5-2012, nº 323/2012, rec. 15/2012 en la que un médico fue condenado inicialmente por un delito de descubrimiento y revelación de secretos en el marco de la actividad de implantación de prótesis mamarias accediendo a numerosas historias clínicas de las pacientes, con el objeto de verificar tipos, marcas y características de los implantes que estaba suministrando la empresa para este tipo de cirugías, ante la existencia de problemas particulares del doctor en relación con determinadas pacientes con el propósito de denunciar a la Empresa para la que prestaba sus servicios.

El Tribunal Supremo estimando su Recurso de Casación se hace eco de su tesis no delincencial y lo absuelve de la vulneración del secreto médico, afirmando entre otros razonamientos: *"La Sala considera concurrente un error de prohibición invencible. El acusado se asesoró, acudiendo a fuentes de su máxima solvencia para desvanecer el error, y actuó en defensa de su propio derecho al ejercicio de su profesión sin el temor de una responsabilidad exigible, y en la creencia, errónea, de que la denuncia que formulaba requería una previa indagación de los hechos .*

... "porque recabó asesoramiento jurídico por lo que estaba convencido que actuaba dentro de la legalidad" y... "el error es invencible e inevitable cuando el sujeto se ha visto apoyado por representantes del Ministerio Fiscal"

En otro orden de cosas, en el ámbito civil, destaca la ST de la Sala 1ª del TS de 27 de Enero de 1997, por la que se condena por daños morales a la Comunidad de Madrid en su condición de titular de un Hospital de Madrid por la pérdida de una HC y el

uso posterior difamatorio contra el paciente de sus datos del historial médico. En esta sentencia se verifica la titularidad compartida del Hospital y del paciente.

Para finalizar este apartado de jurisprudencia penal en relación con los delitos de descubrimiento y revelación de secretos médicos es destacable la STS del Tribunal Supremo de 23/Septiembre/2.015 que básicamente confirma la de la Audiencia de Baleares de 16 de Febrero del 2.015 en la que se condena a un médico a DOS AÑOS, SEIS MESES Y UN DÍA de privación de libertad, MULTA de diecisiete meses a razón de quince euros diarios, con responsabilidad personal subsidiaria en caso de impago, inhabilitación absoluta por tiempo de seis años y al abono de las costas procesales". Su conducta fue que, aprovechando tal condición, consultó el historial clínico de varios compañeros sin su consentimiento, obteniendo así información clínica especialmente protegida hasta un total de 25 ocasiones.

Igualmente es resaltable la condena confirmatoria del TSJ de Navarra a una indemnización de 125.000 Euros a los familiares de una chica fallecida en Pamplona, por un acceso masivo a su historia clínica ordenando además retirar las fotografías de la HC de la misma, ni aún cuando numerosos accesos se realizaron con fines terapéuticos de cara a otros casos clínicos, pero con no fines asistenciales, ni con consentimiento ni de la paciente, ni de los familiares. Como vemos la protección a la intimidad personal, alcanza de modo relevante también a la intimidad familiar. Destaca la sentencia que confirma la del Juzgado de lo Contencioso nº 1 de Pamplona de 25-5-11 que de hecho, precisa, que hubo 2.825 accesos a estas fotografías, realizados por 417 usuarios integrados en 55 servicios y procedentes de todos los centros sanitarios, cuando la paciente "sólo estuvo en un hospital y en 4 servicios".

**EL SECRETO PROFESIONAL:
CONCEPTO Y REGULACIÓN
DEONTOLÓGICA Y JURÍDICA**

Mariano Casado Blanco

Presidente de la Comisión de Deontología del ICOMBA.

Profesor de Medicina Legal UEX

INTRODUCCIÓN.

El Secreto Médico, como variante del Secreto Profesional, se configura como una de las señas de identidad que ha caracterizado el ejercicio de la Medicina a lo largo de su historia. Debe ser tal el sentir ético del médico con respecto al secreto que se le considera como una condición esencial e inseparable de la profesión médica y uno de *“los pilares en los que se fundamenta la relación médico-paciente”*, tal y como indica el artículo 27.1 del Código de Deontología Médica.

Esta relación está *“basada en la mutua confianza”*, y hace que el paciente deposite en el médico sus intimidades, temores, hechos y circunstancias relativas a su biografía, que en muchas ocasiones no las conocen ni sus más próximos o allegados. En contrapartida, el médico debe mostrarse especialmente prudente con respecto a la protección de esos datos que, de una u otra manera, conoce de su paciente.

La Real Academia Española, define *“secreto”* como aquello *“que, cuidadosamente, se tiene reservado y oculto”*. Esta definición envuelve cualquier cosa que se conozca de otra persona, incluyendo lo puntual y lo que se ha conocido a lo largo del tiempo, pero que debe estar bajo el control de la prudencia y alejado del conocimiento general.

Cuando estas cuestiones las trasladamos al campo profesional, se establece el denominado Secreto Profesional, considerado simultáneamente como un deber del profesional y como un derecho del ciudadano.

Por su parte el Secreto Médico como forma particular o variedad de secreto profesional, como ya se ha indicado, tiene un origen que se remonta al mismo Juramento Hipocrático, donde se establecía la obligación moral del médico de mantener en secreto los datos revelados por parte de su paciente: *“lo que en el ejercicio de la profesión y aun fuera de ella viere u oyere acerca de la vida de las personas y que no deba ser revelado, callaré considerándolo secreto”*.

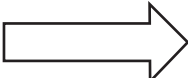
La existencia de este Juramento y de su poder vinculante trae su razón de ser en el principio de confianza y de fidelidad que sustentan la relación médico-paciente. Esta enunciación básica, que satisfacía la obligación de secreto con el simple *“no decir”*, se encuentra hoy muy superada y precisa de matizaciones, que posteriormente analizaremos y sin las cuales queda incompleta.

Es preciso dejar constancia, como bien afirma Siso Martín, de que esta relación (bilateral), conformada entre un médico y un paciente, recibe consecuencias, en caso de quebrantamiento de las obligaciones que contiene, que alcanzan al con-

texto social y de un modo indirecto afectan al interés general por estar inserta, dicha relación, en el terreno del bien común. Si el paciente no puede confiar en su médico es la relación social general, en definitiva, la que se resiente y esta situación puede generar problemas que afecten a la población en su conjunto, que no transmite la información relativa a su salud a los profesionales y no obtiene, con ello, el resultado del trabajo de aquellos. Es inevitable el recordar a Laín Entralgo cuando afirmaba que en la quietud del gabinete del médico con su paciente, en realidad hay tres elementos: los dos expresados y la sociedad en su conjunto.

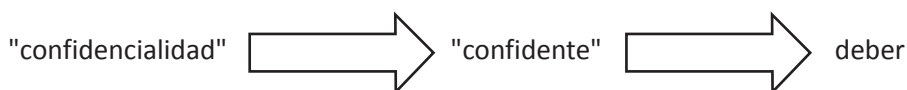
Pero como se decía al inicio del tema, es preciso saber de lo que estamos hablando para poder tener una opinión al respecto y no enmarañar los conceptos. Por ello antes de analizar el Secreto Médico, conocer su regulación y saber de sus limitaciones, bueno será diferenciar conceptos que en muchas ocasiones son confundidos, quizás por su cercanía y que hacen referencia a los términos de *"intimidad"*, *"confidencialidad"* y *"secreto"*.

Cuando se habla de *"intimidad"* (de interior *"intimus"*), se refiere a la vida privada de una persona, sus pensamientos, sentimientos, deseos, ideologías, creencias religiosas o cuestiones referidas a relaciones íntimas o incluso actos y circunstancias de carácter fisiológico, que cada ser humano y por diferentes motivos quiere guardar para sí y que sólo lo dará a conocer, a un grupo reducido de personas de su confianza. Por ello, los datos íntimos han de ser respetados para a su vez, respetar la autonomía y libertad personal, pues al violentar la intimidad se violenta la dignidad humana. Es tal la importancia de la intimidad, que hasta la Constitución Española le da la consideración de derecho fundamental.

"intimidad"  derecho.

Con esto, se podría plantear la cuestión de qué datos se pueden considerar íntimos. Para ello es interesante la definición que da Ataz López, indicando que son *"aquellos que afecten a la vida privada de una persona o de una familia, sobre los que el común sentir social, o el propio interesado, considere que no deben de ser revelados y que se hayan conocido en el ejercicio de la profesión; siempre que, por supuesto, se trate de datos secretos, ya que no parece que pueda considerarse violación del Secreto Médico cuando se revele un dato que es notorio"*.

Por otro lado, cuando se hace mención de la *"confidencialidad"*, se debe entender como una actitud o comportamiento obligatorio de respeto, de silencio, de secreto derivado de la propia esencia del hecho o dato íntimo o privado, por parte de la persona que lo conoce. Cuando un dato que corresponde a la intimidad de una persona y ese es conocido por otra persona, bien por revelación o por otro medio, esta persona está en posesión del conocimiento de dicho dato íntimo, y por tanto adquiere la condición de *"confidente"* y se convierte en un deber para ese que conoce o sabe de dicho dato íntimo.



A modo de ejemplo se puede indicar que si alguien facilita datos de una historia clínica sin la debida autorización o incluso accede a la misma en situación similar, estará cometiendo una violación de la intimidad del paciente a quien corresponde la historia clínica y la persona que haya accedido a la misma incurrirá en un infracción del deber u obligación de confidencialidad.

Aunque también hay que señalar que la confidencialidad existe exclusivamente tanto en función de determinadas circunstancias como mientras no haya un interés superior que obligue a su puesta en conocimiento, siguiendo así la teoría del Secreto Médico relativo. Así y continuando con el mismo ejemplo, los datos de la historia clínica deberán ser mostrados en caso de una presunta valoración de praxis médica o bien ante la redacción de un Informe de alta médica.

Secreto médico compartido y derivado

En medicina el Secreto Profesional es un deber, que debe ser asumido de manera compartida o derivada por todos los profesionales que participan en la atención de la persona. Hasta hace poco, la relación médico-paciente se fundamentaba en su carácter estrictamente bilateral, en el que sólo se relacionaban médico y paciente, sin que otras profesionales estuvieran relacionadas con este pequeño círculo.

Actualmente la asistencia se ejerce por equipos profesionales que necesitan compartir la información para poder dar al paciente una atención de calidad y donde los datos se recopilan de forma más o menos mecánica y por diferentes profesionales tanto sanitarios como no sanitarios que tienen acceso a dichos datos y todos ellos

sujetos al secreto y aparecen los conceptos de “secreto médico compartido” y de “secreto médico derivado”.

Esta ampliación del concepto de secreto médico deriva necesariamente de la asistencia ejercida por un equipo que pueda llegar con más garantías a un diagnóstico, pronóstico y tratamiento y tanto los diversos médicos como el personal de enfermería, laboratorio, farmacia, fisioterapia, terapeutas ocupacional, auxiliares, estudiantes de medicina o enfermería, etc., tienen inexcusablemente el citado deber de “secreto médico compartido”. Es por tanto una derivada necesaria de la medicina moderna, muy amplia y tecnificada.

Pero igualmente, emergen otros factores sobreañadidos al proceso asistencial, tales como las labores de gestión y administración (personal de justicia, compañías aseguradoras, riesgos laborales, certificaciones de calidad, etc.) que obligan a que otro tipo de personal no sanitario, puedan tener acceso a la documentación clínica o a los datos de un paciente, dando lugar a otro tipo de secreto que se conoce como “secreto médico derivado”.

REGULACIÓN JURÍDICA O LEGAL DEL SECRETO MÉDICO:

Aunque desde el punto de vista legislativo no hay normas específicas que regulen el secreto profesional en general ni el secreto médico en particular, sí hay reseñas en distintos textos en las que se puede determinar que no se trata de una “mera” obligación legal del médico, sino de un aspecto substancial del acto médico, que trata nada menos que de la protección del derecho del paciente a la intimidad.

Para analizar esta Regulación, se establece el siguiente esquema:

1.- Normativa Civil y Administrativa:

A) Estatal.

B) Autonómica.

2.- Normativa Penal.

A) Código Penal.

B) Ley de Enjuiciamiento Criminal.

3.- Normativa Deontológica.

A) Código de Deontología Médica.

1.- NORMATIVA CIVIL Y ADMINISTRATIVA:

A) Normativa Estatal:

Constitución Española:

El artículo 24.2, en su inciso final, indica que: *"la ley regulará los casos en que, por razón del parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos"*.

Esta previsión constitucional que hace referencia al Secreto Profesional, no ha sido objeto de cumplimiento mediante la oportuna y anunciada ley reguladora.

Igualmente la propia Constitución reconoce la protección de la intimidad de la persona como un derecho fundamental y el artículo 18.1 establece las garantías respecto al *"derecho al honor, a la intimidad personal y familiar y a la propia imagen"*.

Como consecuencia de ello y en el ámbito privado, este derecho comenzó a fundamentarse de forma activa con la entrada en vigor de la *Ley 1/82, de 5 de mayo de 1982*, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, donde se considera como irrenunciable, inalienable e imprescriptible (artículo 1.3), y aunque no hace referencia específica al Secreto Médico, sí que establece la figura de la intromisión ilegítima cuando se revelan datos privados de una persona, que han sido conocidos a través de la actividad profesional y considerándola, por otro lado, legítima cuando esté expresamente autorizada por ley o cuando el titular del derecho haya concedido al efecto su consentimiento expreso (artículo 2.2).

Del mismo modo, la *Ley General de Sanidad, de 25 de abril de 1986*, reconocía el derecho al respeto de la Intimidad y a la Confidencialidad.

Entre los derechos de los ciudadanos respecto de las administraciones sanitarias recogía, en su artículo 10, el de la Confidencialidad respecto de la información relativa a su proceso e incluso a su estancia en centros sanitarios.

Y en el artículo 61 de dicha norma se plasmaba el deber de reserva respecto de la información que contienen las historias clínicas.

Así y de forma textual se citaban como derechos la *"confidencialidad de toda la información relacionada con su proceso y su estancia"* (artículo 10.3). Además la obligación de *"... quedar plenamente garantizados el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quién, en virtud de sus competencias, tenga acceso a la historia clínica"* (artículo 61).

Posteriormente, tanto la *Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)*, con la modificación de 5 de marzo de 2011, como el *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/99, de 13 de Diciembre, de Protección de Datos de Carácter Personal y el Real Decreto 195/2000*, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11-6-1999, en todos ellos establecía como una obligación la protección de los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) pero admitiendo el acceso de los profesionales sanitarios a la información de sus pacientes y estableciendo la regulación al respecto.

De ahí que se instaurara la necesidad de reglamentar tanto la recogida como el tratamiento de datos médicos derivados de la investigación médica, gestión hospitalaria, sanidad pública e incluso salud laboral, garantizando el carácter confidencial y la seguridad de los datos de naturaleza personal referidos a la salud, aparte de velar porque se haga uso de los mismos dentro del respeto a los derechos y libertades fundamentales del individuo y sobre todo el derecho a la privacidad.

Interesante es tener en cuenta que cuando se hace referencia a la protección de datos, estos no deben quedar limitados a los "íntimos", sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto es la protección de todos los datos de carácter personal. Por tanto no tan solo son los datos de la vida privada o íntima de la persona, sino que se amparan todos los que identifiquen o permitan la identificación de la persona, pudiendo servir para la obtención de su perfil privado o para otra utilidad que en determinadas circunstancias pudiera constituir una amenaza para el individuo.

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, convertido actualmente en el texto de referencia en materia de derechos y obligaciones de los pacientes, expresa claramente la obligación de los centros sanitarios de preservar la información que poseen de sus pacientes (confidencialidad) y restringir el acceso exclusivamente a los supuestos permitidos por la ley.

Acoge la necesidad de reconocer los derechos de los pacientes, entre los que figuran el derecho a la información, el consentimiento informado y la intimidad (capítulo III del citado texto legal) de la información relativa a la salud de las personas y establece

que, el Sistema Nacional de Salud, debe asegurar en condiciones de estricto respeto la intimidad personal y la libertad individual del usuario, garantizando la confidencialidad de la información relacionada con los servicios sanitarios que se prestan y sin ningún tipo de discriminación.

Precisamente en su artículo 7 referente al derecho a la intimidad indica que:

1. *“Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley”.*
2. *“Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes”.*

Hay otras Normas Legales concretas del ámbito médico-sanitario que hacen referencia al secreto y a la confidencialidad.

a) En materia de extracción y trasplantes de órganos:

- La Ley 30/1979, de 27 de octubre, sobre extracción y trasplante de órganos establecía los requisitos para la cesión, extracción, conservación, intercambio y trasplante de órganos humanos con fines terapéuticos, y fue desarrollada por el Real Decreto 426/1980, de 22 de febrero, sobre extracción y trasplante de órganos, que regulaba las condiciones del personal y los centros sanitarios y los principios éticos que debían seguirse en la donación en muerte encefálica y el trasplante de órganos.

Los progresos científicos y técnicos llevaron a una derogación de dicho desarrollo por el Real Decreto 2070/1999, de 30 de diciembre, por el que se regulan las actividades de obtención y utilización clínica de órganos humanos y la coordinación territorial en materia de donación y trasplante de órganos y tejidos, el cual incorporaba novedades como la donación tras la muerte por parada cardiorrespiratoria, con implicaciones en la preservación, los avances tecnológicos en el diagnóstico de la muerte encefálica o el funcionamiento de las organizaciones estatales y autonómicas dedicadas a la coordinación, el rápido intercambio de información y la supervisión y evaluación de las actividades, habida cuenta de la creciente complejidad organizativa.

La Directiva 2010/53/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, sobre normas de calidad y seguridad de los órganos humanos destinados al trasplante, disponía una serie de requisitos mínimos que deben aplicarse a la donación,

evaluación, caracterización, obtención, preservación, transporte y trasplante de órganos humanos destinados a trasplante, con el fin de garantizar altos niveles de calidad y seguridad de dichos órganos. Entre los mismos se incluyen la designación de autoridades competentes, el establecimiento de criterios nacionales de autorización de centros, el desarrollo de un marco de calidad y seguridad que comprenda los protocolos necesarios para el desarrollo efectivo del proceso, la cualificación de los profesionales implicados y la aplicación de programas de formación específicos. La mencionada directiva asimismo impone requisitos de trazabilidad y el desarrollo de un sistema para la notificación y gestión de eventos y reacciones adversas graves, dispone los datos mínimos que deben recabarse para la evaluación de donantes y órganos y obliga al establecimiento de sistemas de información y a la realización de informes periódicos de actividad. Entre sus fundamentos éticos destacan los relacionados con la voluntariedad y la gratuidad, el consentimiento, la protección del donante vivo y la protección de datos personales.

Real Decreto 1723/2012, de 28 de diciembre, por el que se regulan las actividades de obtención, utilización clínica y coordinación territorial de los órganos humanos destinados al trasplante y se establecen requisitos de calidad y seguridad.

Esta última referencia establece en su artículo 4, sobre *Principios fundamentales que rigen la obtención y la utilización clínica de los órganos humanos*.

1. En la obtención y la utilización de órganos humanos se deberán respetar los derechos fundamentales de la persona y los postulados éticos que se aplican a la práctica clínica y a la investigación biomédica.
2. Se respetarán los principios de voluntariedad, altruismo, *confidencialidad*, ausencia de ánimo de lucro y gratuidad, de forma que no sea posible obtener compensación económica ni de ningún otro tipo por la donación de ninguna parte del cuerpo humano.

b) En materia de medicamento y receta médica:

Tanto la *Ley 25/1990, de 20 de diciembre, del Medicamento* como la *Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios*, establecen las debidas garantías de respeto a los postulados éticos.

Y lo mismo ocurre en cuanto a la receta médica está regulada legalmente por el *Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación* y por el *Real Decreto 81/2014, de 7 de febrero*.

c) En materia de interrupción voluntaria del embarazo:

La Ley Orgánica 2/2010 de interrupción voluntaria del embarazo, establece en su preámbulo la vinculación de la sexualidad y la procreación con valores y derechos fundamentales de nuestro ordenamiento, como la dignidad de la persona, el libre desarrollo de la personalidad o los derechos a la intimidad y a la confidencialidad.

d) En materia de Técnicas de Reproducción Asistida:

Ley 14/2006, de 26 de mayo, sobre técnicas de reproducción humana asistida, en su artículo 3.6, se establece que "todos los datos relativos a la utilización de estas técnicas deberán recogerse en historias clínicas individuales, que deberán ser tratadas con las debidas garantías de confidencialidad respecto de la identidad de los donantes, de los datos y condiciones de los usuarios y de las circunstancias que concurran en el origen de los hijos así nacidos. No obstante, se tratará de mantener la máxima integración posible de la documentación clínica de la persona usuaria de las técnicas".

e) En materia de Ensayos clínicos:

Real Decreto 223/2004, de 6 de febrero, por el que se regulan los ensayos clínicos con medicamentos; que garantiza la estricta confidencialidad a las partes en un ensayo clínico y protege la información relativa al mismo del acceso por terceros no autorizados.

Así en su artículo 3.2 indica que: "Los ensayos clínicos se realizarán en condiciones de respeto a los derechos del sujeto y a los postulados éticos que afectan a la investigación biomédica con seres humanos. En particular, se deberá salvaguardar la integridad física y mental del sujeto, así como su intimidad y la protección de sus datos, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

B) Normativa Autonómica:

a) *Ley 12/2001 de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid.* En dicho texto y más concretamente en el Título IV y referido a "Derechos y Deberes de los ciudadanos", se incorpora una completa y extensa regulación acerca de la posición jurídica de los ciudadanos ante el sistema sanitario madrileño, que se traduce en el reconocimiento de un amplio catálogo de derechos, una relación de deberes de los mismos, así como las garantías necesarias para dotarlos de efectividad.

Concretamente el artículo 27.3 establece que: *"El ciudadano tiene derecho a mantener su privacidad y a que se garantice la confidencialidad de sus datos sanitarios, de acuerdo a lo establecido en la legislación vigente".*

b) *Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas, donde recomendaba sobre la necesidad de ir implantando protocolos de actuación para garantizar que la confidencialidad de los datos de salud no se vea vulnerada por personas no autorizadas, para evitar que esta información y documentación pudiera ser cedida a terceros sin las debidas garantías y previsiones legales para establecer medidas de custodia y archivo.*

2.- NORMATIVA PENAL.

A) Código Penal:

En principio hay que tener presente que en la última reforma del Código Penal, que entró en vigor el día 1 de julio de 2015 (*L.O. 1/2015, de 30 de marzo*), se han modificado determinados artículos del anterior Código Penal (CP), que estaban regulados por la Ley Orgánica 10/1995, de 23 de noviembre.

En lo que respecta al tema que estamos tratando, el Título X del CP; *“Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”* (arts. 197-201), incluye como figuras delictivas:

- Apoderarse de información reservada de otra persona.
- Alterar o modificar la información en perjuicio de tercero.
- Difundir, ceder o revelar la información anteriormente citada
- Tener, el autor del delito, la condición de responsable de los ficheros
- Tratarse de datos sensibles o ser su titular menor o incapaz. Los datos de salud se consideran siempre información sensible.
- Existir un móvil lucrativo en la acción delictiva.
- Autoridad o funcionario público que prevaliéndose del cargo divulgue la información fuera de los casos permitidos por la ley.
- La persona que por su profesión u oficio conozca y revele indebidamente la información reservada.

Además introduce como novedad una nueva figura delictiva, que hace mención al *“delito contra la intimidad”*. Los supuestos, que tienen interés en el mundo médico, son aquellos en los que las imágenes o grabaciones de otra persona se obtienen con

su consentimiento, pero son luego divulgados contra su voluntad, cuando dicha imagen o grabación se haya producido en un ámbito personal y su difusión, insistimos, sin el consentimiento de la persona afectada, lesione gravemente su intimidad.

Trata de proteger la intimidad personal en relación con materiales fotográficos o audiovisuales cuya difusión puede generar un menoscabo grave. La conducta se construye sobre una primera fase en la que el material se obtiene con consentimiento del afectado y sobre una segunda fase en la que la difusión se produce sin tal consentimiento.

B) Ley de Enjuiciamiento Criminal:

Este texto legal obliga al médico a declarar los hechos que supuestamente sean delictivos. Así el artículo 262 dispone que: *“Los que por razón de sus cargos, profesiones u oficios tuviesen noticia de algún delito público estarán obligados a denunciarlo inmediatamente al Ministerio Fiscal, al Tribunal competente o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante”*.

3.- NORMATIVA DEONTOLÓGICA.

A diferencia de lo que ocurre con la Normativa General, en el Código de Deontología Médica de la Organización Médica Colegial (OMC), y concretamente en su capítulo V, (artículos 27 a 35) queda regulado ampliamente el Secreto Médico, indicando que tal obligación lo es para todos los médicos, con independencia de *“cualquiera que sea la modalidad de su ejercicio”*.

Para ello establece que *“el secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica”* (art. 27.2), e incluso indica que *“la muerte del paciente no exime al médico del deber de secreto profesional”*. (art. 28.5)

Con respecto al Secreto médico compartido y derivado, indica que:

“El médico debe exigir a sus colaboradores sanitarios y no sanitarios absoluta discreción y observancia escrupulosa del secreto profesional” (artículo 29.1).

“En el ejercicio de la medicina en equipo, cada médico tiene el deber y responsabilidad de preservar la confidencialidad del total de los datos conocidos del paciente” (artículo 29.2).

“El médico debe tener una justificación razonable para comunicar a otro médico información confidencial de sus pacientes” (artículo 29.3).

No olvida el Código el hecho de la informatización de los datos y a este respecto quedan regulados en 3 apartados correspondientes al artículo 27:

Artículo 27.4 *“En las instituciones sanitarias informatizadas los médicos directivos velarán por una clara separación entre la documentación clínica y la administrativa”.*

Artículo 27.5 *“El médico no puede colaborar en ninguna base de datos sanitarios si no está garantizada la preservación de la confidencialidad de la información depositada en la misma”.*

Artículo 27.6 *“El médico podrá cooperar en estudios epidemiológicos, económicos, de gestión, etc., con la condición expresa de que la información en ellos utilizada no permita identificar ni directa ni indirectamente, a ningún paciente”.*

E incluso el Código de Deontología, en su artículo 28, recoge la conducta a seguir en determinadas circunstancias derivadas de necesidades docentes e investigadora:

Artículo 28.1, *“el director médico de un centro o servicio sanitario velará por el establecimiento de los controles necesarios para que no se vulnere la intimidad y la confidencialidad de los pacientes ni la documentación referida a ellos”.*

Artículo 28.2, *“el médico procurará que en la presentación pública de documentación médica en cualquier formato, no figure ningún dato que facilite la identificación del paciente”.*

Artículo 28.3, *“está permitida la presentación de casos médicos que hayan sido fotografiados o filmados para fines docentes o de divulgación científica habiendo obtenido la autorización explícita para ello o conservando el anonimato”.*

CIRCUNSTANCIAS EN LAS QUE EXISTE OBLIGACIÓN DE REVELAR EL SECRETO PROFESIONAL DEL MÉDICO.

Sin lugar a dudas que el manejo de la confidencialidad en el trabajo clínico diario es un asunto mucho más privativo de la ética profesional que de las exigencias legales e incluso el uso de la información sanitaria fuera del marco estrictamente asistencial requiere de una serie de precauciones que permitan hacer efectivo el respeto a los derechos del propio paciente.

El Código de Deontología Médica (artículo 30.1) establece que: *“el secreto profesional debe ser la regla. No obstante, el médico podrá revelar el secreto exclusivamente, ante quien tenga que hacerlo, en sus justos límites, con el asesoramiento del Colegio si lo precisara, en los siguientes casos”*:

- En las Enfermedades de declaración obligatoria (EDO):

Quizás sea uno de los motivos de revelación que tengan mayor justificación, ya que está en juego un bien mayor, como es la salud de otras personas. A pesar de ello algunos autores no lo consideran como revelación sino más bien una transmisión de datos. Sea cual sea su consideración, el Sistema de Enfermedades de Declaración Obligatoria (EDO) constituye uno de los sistemas básicos de la Red de Vigilancia Epidemiológica, de acuerdo con lo dispuesto en el artículo 8 del Real Decreto 2210/1995, de 28 de diciembre, por el que se creó la referida Red. Su finalidad es contribuir a la prevención y control de las enfermedades incluidas en las listas de declaración obligatoria tanto estatales como autonómicas. Este imperativo le corresponde realizarlo, de forma exclusiva, a los médicos ya ejerzan en el sector público o en el privado.

nota: Para ampliar este apartado les derivo a mi libro "Valoración médico-legal de la documentación sanitaria") (Recordar que las EDO están reguladas por la Orden SSI/445/2015, de 9 de marzo, por la que se modificaron los anexos I, II y III del Real Decreto 2210/1995, de 28 de diciembre, relativos a la lista de enfermedades de declaración obligatoria.

Los dilemas éticos que estas situaciones pueden generar, van más allá de la simple obligación de declarar, ya que se pueden generar una serie de conflictos de intereses. El más relevante es el que se plantea acerca de si es obligado informar a las personas allegadas a un paciente portador de una enfermedad infecto-contagiosa y que puede contagiarlas. El planteamiento ético es si deben primar o no el preservar la salud de terceros o la salud pública frente al derecho a la intimidad del paciente.

Como solución práctica en el caso de que se tenga la evidencia de que hay un peligro real de contagio para un tercero, y siempre que el paciente no esté dispuesto a comunicar personalmente su situación y/o a tomar medidas preventivas adecuadas, el médico puede y debe revelar el secreto, amparándose en un estado de necesidad y reforzando el derecho de información de las personas que, por su convivencia con

el paciente, corren riesgo de ser contagiadas. *“Si el paciente se negare a ello, el médico tiene la obligación de intentar convencerlo, advirtiéndole que, si persiste en su negativa, será el mismo médico quien lo haga.”*

Se podría contemplar un quebrantamiento del secreto médico, para aquellos casos en que el peligro sea remoto o poco probable. Por ello, cada caso deberá ser evaluado conforme al criterio particular de la colisión de intereses, siendo el propio médico el que evaluará si existe o no justa causa para su revelación.

Idéntica situación se puede dar en el ámbito laboral, por ejemplo sobre los datos relativos al paciente VIH. En este contexto hay que tener presente que la realización de estas pruebas de detección conlleva la necesidad del previo consentimiento, y caso de realizarse sin consentimiento se podría incurrir en atentado a la integridad e intimidad la persona. Caso de detectarse una seropositividad, no existe exigencia legal de comunicarla al empresario ni al resto de compañeros. En estos casos si es recomendable comunicarlo a los servicios médicos de la empresa, los cuales están obligados en el secreto profesional con todas sus consideraciones.

- En las certificaciones médicas:

Los médicos tienen la obligación legal de certificar el estado de salud de un paciente incluida la muerte, considerando su saber científico y el cumplimiento de las normas jurídicas y profesionales marcadas por la pericia, la diligencia y la prudencia. Se trata de un acto médico por el que este da un testimonio cierto, verídico y preciso acerca de un hecho. Aunque su finalidad no es asistencial, se relaciona con el cumplimiento de una obligación con implicaciones jurídicas o legales. La petición de certificado médico se efectúa porque el ordenamiento jurídico indica una necesidad del ciudadano para optar a determinados servicios y actividades o acreditar situaciones civiles destacadas (nacimiento, defunción, entre otros). Los certificados médicos oficiales, no suelen presentar dificultades a menos que el médico oculte o falsee deliberadamente alguna cuestión de trascendencia.

Es más si se revisa el documento de Certificado Médico Oficial, se puede apreciar como en el último párrafo se indica que la certificación se hace a *“instancias del...”* o a petición del interesado, por lo que el médico que certifica queda liberado por el propio interesado del deber de secreto profesional.

- Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo:

Es una temática complicada en que la decisión de revelar el secreto debe decidirla el propio médico. Una posibilidad nada problemática es solicitar permiso al paciente para hacer uso de la información. El dilema se produce cuando el médico no dispone de autorización entonces es preciso que la actuación médica esté justificada suficientemente o basada en datos objetivos y que el mal causado no sea mayor que el que se trate de evitar. Como ejemplo un paciente diagnosticado de enfermedad de transmisión sexual y se niega informar a su pareja. El conflicto deontológico que se plantea, se centra en el respeto del derecho del paciente a la confidencialidad y al derecho a la protección de la salud de su pareja, extensible incluso a terceras personas no identificables e incluso referido al tema de salud pública.

- Cuando se vea injustamente perjudicado por mantener el secreto del paciente y éste permita tal situación:

Es imposible garantizar la confidencialidad absoluta y aunque en el secreto médico tiene primacía el bien jurídico de la intimidad del paciente sobre los intereses del médico, ante posibles conflictos o colisión de deberes podrán resolverse a través de la aplicación del criterio de estado de necesidad o de cumplimiento de un deber.

- Aunque el paciente lo autorice, el médico procurará siempre mantener el secreto por la importancia que tiene la confianza de la sociedad en la confidencialidad profesional:

El médico queda liberado del compromiso del secreto por consentimiento expreso del paciente, siempre que este haya sido otorgado de forma válida. Se plantean dilemas en cuanto a la determinación del objeto del consentimiento, pues es el paciente el que determina con su consentimiento el campo de actuación dentro del cual podrá desenvolverse lícitamente el médico. Sin embargo como establece el propio Código dicha autorización no debe perjudicar la discreción del médico, que procurará siempre mantener la confianza social hacia su confidencialidad.

- Por imperativo legal:

1.- En el parte de lesiones,

Todo médico viene obligado a enviar al juez cuando asiste a un lesionado. El médico está obligado a denunciar posibles actos delictivos (lesiones, malos tratos o acciones dentro de las agresiones sexuales) que conozca en su actuación profesional, así lo indica la Ley de Enjuiciamiento Criminal, que establece el deber general de denunciar posibles delitos por parte de aquellos que por razón de su profesión tuvieron conocimiento (artículo 262).

Del mismo modo en su artículo 355, se refiere al personal facultativo y especifica que *“si el hecho criminal que motivare la formación de una causa cualquiera, consistiere en lesiones, los médicos que asistieren al herido están obligados a dar parte...”*. De esta forma el médico deberá revelar datos en relación a la correcta descripción de las lesiones, al tratamiento realizado y evaluación de su pronóstico. Deontológicamente, entre el secreto profesional y el interés general de perseguir el delito, prima este último pero sin olvidar que aún así sigue presente el compromiso del médico hacia sus pacientes, lo que implica el deber moral de secreto. Por ello, el contenido del parte de lesiones debe quedar limitado a lo estrictamente necesario y relevante para el objetivo judicial.

2.- Cuando actúe como perito, inspector, médico forense, juez instructor o similar:

Se trata de un acto médico diferente de la medicina asistencial, y que hace referencia a la medicina pericial. Aún así, el médico no pierde su condición de profesional y sus actos deben ajustarse a la ética médica, incluyendo el deber de secreto. Las diferencias, son claras, según el ámbito en que se desarrolle el procedimiento, ya sea judicial, administrativo o colegial. Siempre será una constante que el informe pericial médico ha de ser justo, ponderado y objetivo. Los dilemas que pueden aparecer en el campo pericial no suelen ser de una vulneración voluntaria del secreto, sino más bien de una resistencia a revelar las confidencias aportadas o conocidas del propio paciente.

En la actuación del médico perito el secreto médico no se establece con las autoridades administrativas, judiciales o colegiales que hayan solicitado el informe. No obstante, tanto si el paciente acude de forma voluntaria como si la prueba ha de practicarse sin su consentimiento o incluso con oposición o indiferencia, el médico debe proceder a dar información acerca de la prueba a realizar así como de su con-

dición (perito, testigo, inspector, médico forense, juez instructor) y prevenirle de alguna manera del no mantenimiento de obligación del secreto profesional de aquello que se obtenga de su relación médico-paciente.

3.- *Ante el requerimiento en un proceso judicial por presunto delito, que precise de la aportación del historial médico del paciente.*

El derecho a la intimidad de una persona no puede comprometer al bienestar social, que a veces depende de la administración de Justicia. Es evidente que se pueden crear serios dilemas y confrontar legítimos intereses del paciente y del médico relacionados con el secreto médico y con el consentimiento del paciente. La historia clínica es una herramienta fundamental de carácter probatorio en determinar responsabilidades civiles, penales o administrativas. En el uso de la historia en supuestos de investigación judicial que se considere imprescindible la unificación de datos identificativos y clínico-asistenciales, se deberá seguir lo que dispongan jueces y tribunales.

Este criterio general que establece la Ley de Autonomía del Paciente, parece referirse solo a procesos penales, en los que por razones de interés general, hay la obligación, por orden del juez, de entregar la historia. No obstante, la prudencia aconseja solicitar al juez que defina la relación que pueda existir entre los datos de la historia y el objetivo del proceso. Si accede, se podrán entregar los documentos que sean relevantes, garantizando en lo posible, la confidencialidad.

4.- *Medicina del trabajo*

El artículo 31 del Código de Deontología recoge, el Secreto en Medicina del Trabajo.

Artículo 31.1 *“Los resultados de los exámenes médicos exigidos por la ley, deben ser explicados a la persona reconocida. Sólo se informará a la empresa o institución pertinente respecto de la aptitud laboral o de las limitaciones o riesgos para la asignación del trabajo”.*

Artículo 31.2. *“Los resultados de los exámenes practicados en el marco de la vigilancia de la salud se comunicarán exclusivamente a la persona afectada. No obstante, el médico de un centro de medicina preventiva o de medicina del trabajo debe transmitir cualquier resultado que sea útil para el paciente, con su consentimiento, a su médico responsable”.*

En este mismo sentido la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL), establece:

Artículo 22.4 que *“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 serían 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”*.

En otras palabras, el secreto impuesto al médico que efectúa el reconocimiento entraría en contradicción con su deber de comunicación de situaciones de riesgo, tanto para un trabajador concreto, como para el resto de sus compañeros. Sin duda que se trata de una cuestión compleja, en la que el médico tendrá que actuar con mucha prudencia, comunicando de forma oficial los datos controvertidos siempre y cuando la eliminación del riesgo no pueda efectuarse sin violentar la confidencialidad entre médico y paciente.

En lo que respecta a la vigilancia de la salud, entendida como la utilización de una serie de técnicas (encuestas, exploraciones físicas, exploraciones complementarias, etc.) sistematizada y periódica, con el objetivo de conocer o detectar cambios en el estado de salud de un individuo o de un colectivo.

Estas actuaciones profesionales tienen un evidente doble objetivo, tanto individual como colectivo.

Desde la perspectiva individual, persigue promover y preservar la salud de los trabajadores, detectando precozmente los factores de riesgo laborales, tanto los generales como los específicos, las patologías laborales y no laborales que puedan afectar al trabajador, así como identificar a aquellos trabajadores especialmente sensibles a ciertos riesgos.

Desde la perspectiva colectiva pretende detectar riesgos inherentes a un determinado puesto de trabajo o a una determinada actividad.

En cuanto a los resultados de la vigilancia de la salud, tanto la confidencialidad de la información como el tratamiento de los datos relativos a la salud obtenidos a

través de los reconocimientos médicos, aparecen contemplados en los apartados 2 y 4 del artículo 22 LPRL, que regulan la circulación de la información relativa a la salud del trabajador en los reconocimientos médicos. Concretamente en el artículo 22.2 LPRL se indica que las medidas de vigilancia se llevarán a cabo respetando la intimidad y dignidad de la persona del trabajador, así como *“la confidencialidad de toda información relacionada con su estado de salud”* (artículo 22.2 LPRL).

Por tal motivo, deontológicamente, la información sobre las pruebas médicas practicadas y su resultado (información médica personal) sólo deben ser conocidos por parte del trabajador afectado, a quien se le deben comunicar los resultados, los servicios médicos encargados de dicha vigilancia y la autoridad sanitaria. La información a terceras personas, solamente podrá facilitarse únicamente si el trabajador da su consentimiento expreso.

En este sentido se regula la confidencialidad de la información relativa a la salud, estableciendo que el acceso a la información *“se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud”*, prohibiéndose expresamente que *“puedan facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador”* (artículo 22.4 LPRL).

Las conclusiones derivadas de las pruebas médicas practicadas, pueden ser conocidas por sujetos distintos a los enumerados en el párrafo anterior, sin necesidad del consentimiento del trabajador. La regla general encuentra excepción en el párrafo segundo del artículo 22.4 LPRL, en que se indica que *“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 de la prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva”* (artículo 22.4 párrafo 2 LPRL).

En referencia al empresario, este debe quedar excluido del conocimiento del estado de salud del trabajador, habilitándolo únicamente como destinatario de un mero juicio de idoneidad, ya sea relacionado directamente con la salud del trabajador, ya sea en relación con las medidas de protección o prevención aplicadas en la empresa.

BIBLIOGRAFIA

1. Altisent R. Consentimiento informado en Atención Primaria. FMC. 2000;7(3): 135-137.
2. Júdez J, Nicolás P, Delgado MT, Hernando P, Zarco J, Granolleres S. Confidencialidad en la práctica clínica, la historia clínica y la gestión de la información. En Gracia D, Júdez J. *Ética en la práctica clínica*. Madrid: Triacastela. 2004; 75-126.
3. Romeo Casabona M., Castellano Arroyo M. La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica. DS Vol. 1, Núm. 1, Julio-Diciembre 1993.
4. Declaración de la Comisión Central de Deontología “sobre las cualidades del certificado médico y sobre sus diferencias con los partes y los informes médicos. Peculiaridades del certificado médico de defunción”, aprobada por el Pleno del Consejo General el 26 de enero de 2007.
5. Código de Deontología Médica. Guía de Ética Médica. Madrid: OMC, julio 2011.
6. Rubio M. Confidencialidad: el derecho a la intimidad. *Jano*, 2008; 1699: 44-46.
7. Delgado Marroquín MT. Confidencialidad y secreto médico en la consulta del médico de familia. *JANO* 2007; 1654: 44-46.
8. Altisent Trota R, Gállego Royo A., Delgado Marroquín MT. Los códigos de deontología profesional. *AMF*. 2014; 10(11):651-658.
9. Gracia D. *Como arqueros al blanco*. Madrid: Triacastela, 2004; pp. 279-299.
10. Altisent R. Ética, Deontología y Derecho: lógicas diferentes en una misma dirección. *Aten Primaria*. 2007;39(5):225-6.
11. Fundación ABIM, et al. La profesión médica en el nuevo milenio: estatutos para la regulación de la práctica médica. *Med Clín (Barc.)*. 2002;118(18):704-6.
12. Sánchez González. M.A. Intimidad y Confidencialidad. Su concepto y su importancia. I Jornada de protección de datos sanitarios en la Comunidad de Madrid. Madrid 2000. p. 55.
13. Ataz López J. Los médicos y la responsabilidad civil. Montecorvo. Madrid 1985. Página 187.
14. Laín Entralgo, P. (1964): *La relación médico-enfermo*, Madrid, *Revista de Occidente*. [2.ª ed., Madrid, Alianza, 1983].
15. Casado Blanco M. *Valoración médico legal de la documentación sanitaria*. Badajoz, autoedición.

**CONFIDENCIALIDAD, LA CUSTODIA DE LA
HISTORIA CLÍNICA EN MODELO TRADICIONAL
Y EN LA HISTORIA CLÍNICA INFORMATIZADA**

Dr. D. Ceciliano Franco Rubio

Director Gerente del Servicio Extremeño de Salud

1.- CONCEPTO

Definición de Historia Clínica tradicional:

La historia clínica tradicional consiste en una acumulación física, normalmente archivada en carpeta o carpetas, de todos los informes y pruebas realizados a un paciente en todas las actuaciones médicas y sanitarias que le han sido realizadas.

Definición Historia Clínica Electrónica:

La historia clínica electrónica supone incorporar las Tecnologías de la Información y la Comunicación (TIC) en el núcleo de la actividad sanitaria. Esto trae como consecuencia que la historia deje de ser un registro de la información generada en la relación entre un paciente y un profesional o un centro sanitario, para formar parte de un sistema integrado de información clínica.

Historias Clínicas electrónicas en el SNS:

- Andalucía (Diraya)
- Cataluña
- Euskadi (Osabide)
- Galicia (IANUS)
- Navarra (HCI)
- Canarias (Drago)
- Valencia (Abucasis)

2002: transferencias sanitarias

- Asturias: EDESIS (OMI-AP, Selene, Millenium)
- Aragón: SGP (OMI-AP; HP-HIS)
- Castilla la Mancha (Turriano, Mambrino)
- Extremadura (Jara)
- Castilla y León (Medora, Jimena)
- Baleares (eSIAP, HP-HCIS)
- Selene, OMI-AP, HP-HCIS, SAP, Milenium

4.- “HISTORIA” de la HISTORIA CLÍNICA

Las Historias Clínicas más antiguas que se conservan son las incluidas en los libros I y III de las Epidemias del Corpus Hippocraticum.

Hipócrates de Cos (460-377 a.C.), “inventor” de la Historia Clínica, reflejaba en sus relatos tres partes fundamentales:

- descripción del sujeto
- descripción de la enfermedad
- curación o muerte

La Historia Clínica, en tanto en cuanto narración de un acaecer patológico, ha permanecido inmutable a lo largo de los siglos. Las ideas que los Médicos tenían han ido variando pero no la forma de plasmarlo en un pergamino, papiro, papel escrito o sistema informático.

El cambio de mentalidad del hombre del renacimiento hace que la historia clínica se convierta en un relato preciso, objetivo y exento de interpretación doctrinal, acaba con una reflexión diagnóstica y las indicaciones terapéuticas, se hace mención del exitus en el sentido de salida hacia la curación o hacia la mención de la muerte “exitus letalis”. Siguiendo la tendencia de la época, se añade una clara visión estética mejorando el estilo literario y añadiendo coherencia narrativa en la descripción clínica.

A lo largo del s. XIX, gracias a la invención de nuevas técnicas e instrumentos como el termómetro y el estetoscopio, se comenzaron a medir síntomas y signos con precisión, lo que comenzó a enriquecer y hacer más precisas las historias clínicas.

Ya en el siglo XX los continuos avances tecnológicos y médicos hacían cada vez más detallada y voluminosa la información contenida en la historia clínica. Además, se convierte ya en un documento multidisciplinar, no elaborado por un solo médico sino por múltiples profesionales que asisten al paciente.

Durante la segunda mitad del siglo XX comienza la creación de Servicios nacionales de Salud, que proporcionan cobertura sanitaria pública a los trabajadores y con ello la construcción de grandes hospitales. La historia clínica deja de ser entonces propiedad particular del médico ya que se crean los servicios de documentación y custodia, en ellos se archivan ordenados por episodios los contactos del paciente con el sistema público de salud aumentando considerablemente la información contenida en la historia clínica.

Finalmente, con el desarrollo a finales del siglo XX y su total implantación en todos los aspectos de la sociedad en el XXI, se comienza a dar el paso a la informatización y digitalización de la HC.

LEGISLACIÓN

Soporte Legal

Estructuración de la ley

De la general a la autonómica

La Agencia Española de protección de datos interpreta la Ley en modo de Resoluciones y decretos

A la Agencia tiene capacidad sancionadora

Legislación general

- 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 (B.O.E. nº 274 de 15 de noviembre de 2002. Madrid. 2002. 40126-40132), recoge las principales condiciones de la historia clínica en su uso y reglamentación, y la define en su artículo 3 como «el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial».
- La Ley General de Sanidad 14/1986, de 25 de abril, reconoce el derecho del paciente a que quede constancia por escrito de todo su proceso, en una historia clínica, así como a recibir un informe de alta al finalizar su estancia hospitalaria. La historia clínica se identifica por un número único que permite su recuperación rápida en caso de ser necesario un sucesivo proceso asistencial, cause ingreso o no.

Debe estar a estos efectos, en un archivo central y no debe ser sacada del centro asistencial. El Real Decreto 63/1995 (BOE 10-02-95) recoge el derecho del paciente, a petición del mismo, a un ejemplar de su historia clínica o a determinados datos contenidos en la misma. Así mismo, se debe garantizar la custodia de la historia clínica, asegurando la confidencialidad como derecho del paciente. El acceso a la historia clínica sin autorización, con divulgación o adulteración de datos de la misma, viene tipificado como delito en el Código penal (Artículo 292).

- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, define en su artículo 3: “datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables”; en su artículo 7.3, como datos especialmente protegidos recoge: “los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo po-

drán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente”; en el artículo 8, de datos relativos a la salud, expone: «sin perjuicio de lo que se dispone en el artículo 11 sobre cesión y comunicación de datos y el correspondiente consentimiento del paciente, 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 acuda no hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Todas estas normativas implican que la actividad profesional del médico ha experimentado una importante transformación social, marcada especialmente por una nueva forma de relación del médico con el paciente y el conjunto de la sociedad. Todo ello hace que el ejercicio de la medicina se encuentre iluminado por determinadas formalidades e implicaciones legales que obligan al médico a conocerlas y, en cierta manera, a dominarlas. El Código de Deontología Médica-Guía de Ética Médica (CDM), aprobado por la Asamblea General de la Organización Médica Colegial en julio de 2011, dedica múltiples apartados a concretar los diversos aspectos relacionados con la historia clínica.

Legislación autonómica: Extremadura

Por su parte, *la Comunidad Autónoma de Extremadura, en su Ley 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente, especifica que:*

- La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro sanitario.
- La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.
- Todo paciente o usuario tiene derecho a que quede constancia por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos de atención sanitaria.
- La historia clínica tendrá como fin principal facilitar la atención sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico permitan el conocimiento veraz y actualizado del estado de salud.

- Las historias clínicas deberán ser claramente legibles, evitándose en lo posible la utilización de símbolos y abreviaturas y estarán normalizadas en cuanto a su estructura lógica. Cualquier actuación relativa a la atención sanitaria al paciente deberá ser anotada en la historia, indicando la fecha y hora de su realización, y será firmada de manera que se identifique claramente la persona que la realice.

5.- CONFIDENCIALIDAD DE LA DOCUMENTACIÓN CLÍNICA

La confidencialidad es un aspecto clave de la relación entre profesionales sanitarios y pacientes. Supone la cesión del paciente de una parte reservada de sí mismo y los principios éticos de autonomía y no maleficencia están íntimamente ligados con su preservación.

Al ser la historia clínica el documento donde la relación con el paciente queda reflejada, requiere de una protección extraordinaria por la naturaleza especialmente sensible de la información en ella contenida.

Es preceptivo para el profesional que la elabora conocer algunos aspectos básicos de las leyes fundamentales que la regulan en diferentes aspectos.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, califica a los datos relativos a la salud de los ciudadanos como datos especialmente protegidos, estableciendo un régimen singularmente riguroso para su obtención, custodia y eventual cesión.

El Real Decreto 1720/2007, de 21 de diciembre, que desarrolla dicha Ley 15/1999, califica también los datos relativos a la salud como de nivel alto; lo que significa que requieren unas medidas de seguridad especialmente rigurosas.

Uno de los principios básicos de la Ley 41/2002 es que la persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida. Y la citada Ley, recoge entre otros aspectos, el que toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.

El artículo 33 de la Ley 3/2005 especifica que las historias clínicas son documentos confidenciales responsabilidad de la administración sanitaria o entidad titular del centro sanitario, cuando el médico trabaje por cuenta y bajo la dependencia de una institución sanitaria. En caso contrario, la responsabilidad corresponderá al médico que realiza la atención sanitaria.

6.- GESTIÓN Y ACCESO A LA HISTORIA CLÍNICA

El artículo 33 de la Ley 3/2005 especifica que:

- La gestión de la historia clínica será responsabilidad de la unidad de admisión y documentación Clínica, o unidades similares, de manera integrada en un único archivo de historias clínicas por centro sanitario.
- Los profesionales del centro sanitario que realicen el diagnóstico o el tratamiento del paciente tendrán acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.
- Cada centro sanitario deberá establecer el mecanismo que haga posible que, mientras se presta atención sanitaria a un paciente concreto, los profesionales que le atiendan puedan, en todo momento, tener acceso a la historia clínica correspondiente, a efectos del desempeño de sus funciones.
- El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tendrá acceso a las historias clínicas, con absoluta garantía del derecho a la intimidad personal y familiar, en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.
- El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación, de docencia o de información y estadística sanitaria, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en el Real Decreto 1720/2007 de 21 de diciembre que la desarrolla, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento de no separarlos.
- Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica quedará limitado estrictamente a los fines específicos de cada caso.
- El personal de administración y gestión de los centros sanitarios sólo podrá acceder a los datos de la historia clínica relacionados con sus propias funciones, y en todo caso queda sujeto al deber de guardar secreto de los mismos.

- El acceso por otras personas distintas al paciente a la información contenida en la historia clínica habrá de estar justificado por la atención sanitaria de éste, debiendo quedar constancia en la historia clínica de las personas que han tenido acceso a la misma y de su expreso compromiso por escrito de guardar reserva de la información a que han tenido acceso.
- En todos los casos quedará plenamente garantizado el derecho del paciente a su intimidad personal y familiar, por lo que el personal que acceda a esta información guardará el correspondiente secreto profesional.

7.- CONSERVACIÓN

Las medidas derivadas de la legislación reguladora de la conservación de ficheros que contienen datos de carácter personal, son de aplicación a la documentación clínica de las historias clínicas. Si bien la Ley 41/2002 establece la obligación de los centros sanitarios de conservar la documentación clínica, como mínimo, cinco años desde la fecha de alta de cada proceso asistencial, no hay unanimidad al respecto a nivel autonómico. De hecho, la Comunidad Autónoma de Extremadura, según el artículo 34 de su Ley 3/2005, de 8 de julio de, de información sanitaria y autonomía del paciente, indica que:

- *Los centros sanitarios tienen la obligación de conservar la documentación obrante en la historia clínica en condiciones que garanticen su correcto mantenimiento, confidencialidad y seguridad, para la debida atención al paciente, durante al menos quince años contados desde la fecha del alta de cada proceso asistencial.*
- *En cualquier caso la conservación de la documentación clínica deberá garantizar la preservación de la información y no necesariamente del soporte original.*
- *Se conservará indefinidamente aquella información que se considere relevante a efectos preventivos, epidemiológicos, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. En tales casos, siempre que sea compatible con los fines perseguidos, se despersonalizarán los datos al objeto de impedir la identificación directa o indirecta de los sujetos implicados. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente.*
- Los profesionales sanitarios tienen el deber de cooperar en la creación y el mantenimiento de una documentación clínica ordenada que refleje, con las secuencias necesarias en el tiempo, la evolución del proceso asistencial del paciente.

8.- CUSTODIA

Evidentemente la historia clínica debe estar custodiada de forma que se preserven los derechos tanto de paciente como de profesionales. La Ley 41/2002, en su artículo 19, establece que los centros sanitarios deben tener un mecanismo de custodia activo y diligente de las historias clínicas, que permita la recogida, integración, recuperación y comunicación de la información sometida al principio de confidencialidad según los usos de la historia clínica.

La C.A. de Extremadura, completa lo expuesto en dicha ley en cuanto a la custodia de la HC con lo especificado en el artículo 31 de la Ley 3/2005, de 8 de julio de la Comunidad Autónoma de Extremadura, de información sanitaria y autonomía del paciente:

- Al menos en cada centro sanitario, existirá una historia clínica única para cada paciente y en un modelo uniforme, que recogerá los contenidos mínimos fijados en el artículo siguiente, adaptados al nivel asistencial que tengan y la clase de prestación que realicen.
- Cada centro sanitario archivará la historia clínica de sus pacientes, cualquiera que sea 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, así como la autenticidad del contenido de las mismas y su plena reproductibilidad futura. En cualquier caso, debe garantizarse que queden registrados todos los cambios e identificados los médicos y los profesionales asistenciales que los han realizado.
- Los centros sanitarios deben adoptar las medidas técnicas y organizativas adecuadas para proteger los datos personales recogidos y evitar su destrucción o su pérdida accidental, y también el acceso, alteración, comunicación o cualquier otro procesamiento que no sean autorizados.

Además, en su artículo 33, dicha Ley establece también que *la administración sanitaria o entidad titular del centro sanitario*, cuando el médico que realiza la atención sanitaria trabaje por cuenta y bajo la dependencia de una institución sanitaria, o el médico, en caso contrario, *es responsable de la custodia de las historias clínicas y habrá de adoptar todas las medidas necesarias para garantizar la confidencialidad de los datos y de la información contenida en ellas.*

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 Orgánica 15/1999, de

Protección de Datos de Carácter Personal, el Real Decreto 1720/2007 de 21 de diciembre que la desarrolla, y por la Ley 41/2002 Básica reguladora de la autonomía del paciente y de derecho y obligaciones en materia de información y documentación clínica.

En cuanto al punto de vista del paciente, la citada Ley 3/2005, en su artículo 36, especifica que el paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido en su artículo 34.

Custodia Especial

Todas las Historias Clínicas solicitadas por Tribunales de Justicia y también aquellas Historias Clínicas que considere la Dirección Médica recibirán un tratamiento de especial custodia.

Estas Historias Clínicas serán guardadas en un armario especial cerrado con llave, localizado en las dependencias de la Dirección Médica y el acceso a ellas será expresamente autorizado por ésta; siendo por tanto la Dirección Médica la responsable oficial de su custodia..

9.- MEDIDAS DE SEGURIDAD PARA LAS HISTORIAS CLÍNICAS INFORMATIZADAS

Como ya se ha dicho antes, el Real Decreto 1720/2007 de 21 de diciembre que desarrolla la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en los artículos del 89 al 104, especifica que los datos relativos a la salud requieren unas medidas de seguridad de nivel alto (que se añaden a las que especifica también para los niveles medio y bajo) para la conservación y el aseguramiento de la confidencialidad de los mismos. Estas medidas son las siguientes:

9.1.- Medidas de Seguridad de NIVEL BAJO

Funciones y obligaciones del personal.

1. 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.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Identificación y autenticación.

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.

Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

9.2.- Medidas de seguridad de NIVEL MEDIO

Responsable de seguridad

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Auditoria

1. A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditora interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoria siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoria inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoria deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
3. Los informes de auditoria serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

9.3.- Medidas de seguridad de NIVEL ALTO

Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuen-

tren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Registro de accesos.

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.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurren las siguientes circunstancias:
 - a) Que el responsable del fichero o del tratamiento sea una persona física.
 - b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

10.- MEDIDAS DE SEGURIDAD PARA LAS HISTORIAS CLÍNICAS TRADICIONALES

El Real Decreto 1720/2007 de 21 de diciembre que desarrolla la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, diferencia entre los ficheros automatizados (en nuestro caso historias clínicas informatizadas) y ficheros no automatizados (las historias clínicas tradicionales en papel), especificando para los de estos últimos que contengan datos de salud unas medidas de seguridad de nivel alto (que incluyen también las de nivel medio y bajo), en los artículos del 105 al 114, para la conservación y el aseguramiento de la confidencialidad de los mismos. Estas medidas son las siguientes:

10.1 .- Medidas de Seguridad de NIVEL BAJO

Obligaciones comunes.

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:
 - a) Alcance.
 - b) Niveles de seguridad.
 - c) Encargado del tratamiento.
 - d) Prestaciones de servicios sin acceso a datos personales.
 - e) Delegación de autorizaciones.
 - f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
 - g) Copias de trabajo de documentos.
 - h) Documento de seguridad.
2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
 - a) Funciones y obligaciones del personal.
 - b) Registro de incidencias.
 - c) Control de acceso.
 - d) Gestión de soportes.

Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

10.2.- Medidas de Seguridad de NIVEL MEDIO

Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este Reglamento.

Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

10.3.- Medidas de Seguridad de NIVEL ALTO

Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

11.- CONCLUSIONES

- La sociedad de la información y la revolución de las tecnologías de la información y de las comunicaciones también influyen en el ejercicio de la medicina y demás profesiones sanitarias, y en la transformación de la historia clínica.
- Uno de los más importantes derechos del paciente es la confidencialidad de la información que ha facilitado a su médico. Una de las obligaciones más importantes del médico y del resto de profesionales sanitarios o no, es garantizar ese secreto. Los servicios sanitarios deben arbitrar procedimientos que garanticen la seguridad y la confidencialidad de la información clínica.
- Las tecnologías de la información y de las comunicaciones permiten la informatización de la documentación clínica y su accesibilidad a cualquier profesional que deba atender al paciente, mejorando la continuidad de la asistencia.
- La historia clínica informatizada no supone menos garantías de seguridad y confidencialidad que la documentación en papel, pero también exige establecer procedimientos y planes que garanticen esa confidencialidad y seguridad.
- Las medidas de seguridad exigidas legalmente para las historias clínicas informatizadas difieren como es lógico de las exigidas para las historias clínicas tradicionales en papel.
- Todos los avances tecnológicos no deben hacernos olvidar que lo importante sigue siendo la práctica clínica, la relación médico paciente y el contenido de la historia clínica, con independencia de si está o no informatizada.

SEGURIDAD DE INFORMACIÓN CLÍNICA EN LAS BASES DE DATOS

Julio López Ordiales

Fiscal Delegado Provincial de Criminalidad Informática.

Fiscalía Provincial de Badajoz

1.- INTRODUCCIÓN

La digitalización de los datos comerciales, personales, económicos y de todo tipo, es un hecho, todas las áreas de la sociedad se ven afectadas, incluso mi ámbito de trabajo, la justicia. El mundo de la salud no iba a ser menos, un campo en el que el uso de la tecnología para tratar dolencias es, a veces, vital, no podía quedar fuera de esta evolución. La informatización de la historia clínica, que contiene un volumen importante de información altamente sensible relacionada con el ámbito de la intimidad de las personas, los sistemas de acceso a esa historia desde distintos lugares en los que pueda ser necesario para atender a ese paciente y la creación y gestión de bases de datos centralizadas que permitan una ágil gestión de la información, generan en los ciudadanos y en los profesionales inquietud por la seguridad y confidencialidad de esa información. En general nos preguntamos si se puede garantizar que esos datos no llegarán nunca a manos de quien pueda utilizarlos con otros fines que aquellos para los que fueron recogidos: diagnosticar y curar a los pacientes. Las inquietudes sobre la seguridad y confidencialidad de la información clínica digitalizada se pueden sintetizar en tres categorías como señalan José Antonio Garbayo Sánchez y otros¹:

1. Cuestiones Técnicas: ¿Soporta el estado actual de la tecnología todos los requisitos de seguridad que deberían tener este tipo de sistemas?
2. Materias Organizativas: ¿Está la organización sanitaria nacional y autonómica capacitada para gestionar esta información con todas las garantías?
3. Aspectos Legales: ¿Está respaldado legalmente, a todos los niveles, el uso que se hace de todas esas herramientas y sistemas? ¿Estamos los ciudadanos protegidos frente a posibles perjuicios?

Lo cierto y verdad es que las estadísticas mundiales en materia de ataques informáticos a bases de datos señalan como las más atacadas las bases de datos sobre salud, hospitales, servicios públicos, clínicas, consultas médicas, etc...², son los objetivos de los hackers, y aunque los datos obtenidos en si mismos pueden no significar nada

¹ “La seguridad, confidencialidad y disponibilidad de la información clínica”, José Antonio Garbayo Sánchez, Jokin Sanz Ureta, Javier Carnicero Giménez de Azcárate, Carlos Sánchez García, Informes Sociedad española de Informática de la Salud, 2003, pág. 258

² Según un estudio realizado por BakerHostetler en 2015, del total de incidentes relacionados con ataques phishing, hacking y malware fueron la causa del 31% de las amenazas de seguridad de datos. Del total de los ataques recibidos, un 23% se registró en la industria de la salud, seguida de los servicios financieros, que contabilizaron el 18% y de la educación, que registró el 16%.

pero su estudio y control permite acceder a información valiosa no solo para empresas farmacéuticas, aseguradoras o simplemente mafias, sino para administraciones sanitarias públicas y grupos políticos, solo pensemos en el capítulo presupuestario que se dedica a sanidad. La seguridad y confidencialidad de la información almacenada exige, según la mayoría de la doctrina garantizar los siguientes aspectos de la información, previstos en la Ley Orgánica de Protección de Datos (LOPD 15/1999, de 13 de diciembre) en los arts. 4 a 12:

- *Que la información almacenada esté disponible.* Es decir que cuando se necesite, se pueda acceder a ella y utilizarla.
- *Que a la información almacenada solo acceda quien está autorizado para ello y para el uso a que está autorizado.* Se requiere en este caso identificar claramente a la persona a la que se autoriza, a quien se le concede un permiso específico para desarrollar determinadas tareas. Son los denominados procesos de identificación, autorización y asignación de perfiles y roles de usuarios de las bases de datos.
- *Que la información almacenada se mantiene íntegra,* es decir que los datos introducidos en cada proceso no se han transformado durante su almacenamiento, consulta o transporte. Es la característica denominada de integridad.
- *Que quien acceda a los datos no pueda negar haberlo hecho.* Se trataría de acreditar la trazabilidad del usuario de los datos en cada nivel y para cada función. Es la característica de no repudio.
- *Que la organización propietaria de la gestión pueda comprobar quién ha accedido a la información y en qué transacciones ha participado.* De cada acceso se guarda un registro detallado no solo de quién accedió sino de los datos de fecha y hora, servicios a los que ha accedido, etc. Es el proceso de auditoría.

2.- MECANISMOS DE SEGURIDAD

Lo información almacenado en cualquier sistema de Historia Clínica Informatizada debe hallarse protegida frente al acceso no autorizado, destrucción o alteración indebida de los datos e introducción de forma accidental de inconsistencias. La seguridad en los sistemas de información debe contemplar todas las posibles amenazas, imaginables o no, que se identifiquen sobre todos y cada uno de los elementos del sistema: hardware, software, datos, redes, sistemas de comunicación, etc.... El término *seguridad* se refiere a la protección contra el acceso mal intencionado; mientras que por *integridad* nos referimos a la prevención contra una pérdida accidental de la consistencia de los datos.

Entre las amenazas más evidentes se encuentran, como no, el elemento humano, las personas, tanto las que actúan con carácter voluntario como involuntario, y por supuesto las catástrofes, como los incendios e inundaciones.

Como creación humana las bases de datos se han dotado, como paso obligado de seguridad, de reglas que tienden a garantizar los elementos antes mencionados, integridad, disponibilidad, reserva, trazabilidad, etc...; para ello se han elaborado diversas normas. En esta materia, tratándose de datos personales relacionados con la salud personal, existe normativa general LOPD y su Reglamento y normativa específica Ley 41/2002 y Ley 3/2005, esta última en Extremadura. Se trata de diseñar un sistema de seguridad organizado en diversas "capas", *una genérica, las más externa* que vendría determinada por la normativa general de protección de datos personales, *una específica, intermedia*, recogida por las normas concretas relativas a los datos personales relativos a la salud de carácter nacional y autonómico y una, llamemos, *tercera capa, que veremos al final, que denomino disuasoria*, constituida por las normas administrativas y penales sancionadoras de conductas contrarias a la normativa de protección de datos y al derecho a la intimidad personal.

La *capa más externa define y determina el nivel de protección* que deberían tener las bases de datos en función de determinados parámetros recogidos legalmente, y así los arts. 9 LOPD y 79 a 114 del Reglamento (RLOPD Real Decreto 1720/2007, de 21 de diciembre), otorgando un determinado nivel de seguridad, en este caso alto, a la gestión de los datos de salud, estableciendo además de las exigencias de los niveles bajo y medio, otras específicas, sobre todo en materia de almacenamiento de la información, copia o reproducción, acceso a la documentación y traslado de documentación; *la capa siguiente vendría constituida por las normas reguladoras de la base de datos específica* que define los datos a recabar, su tratamiento y posibles cesiones y que en este caso tendrían como marco la Ley 41/2002 (ámbito nacional) y la Ley 3/2005, de 8 de julio, de información sanitaria y autonomía del paciente, (ámbito autonómico extremeño), y es en este nivel donde se integran todas las acciones directas encaminadas a establecer la seguridad de los datos, como se recogen, como y donde se almacenan, quien, como y desde donde se accede, niveles y permisos de acceso, conservación, tratamiento, etc...

Uno de los elementos necesarios y básicos en materia de seguridad es el denominado documento de seguridad. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá 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. Podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fi-

chero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización (art. 88 RLOPD). Es esencial en las auditorias de seguridad y objeto de sanción su carencia.

La seguridad de los datos que forman parte de la historia clínica tiene el nivel más alto posible, nivel alto, tal y como el art. 81-3-a) del RLOPD señala (arts. 101 a 104 RLOPD). Dicho nivel de protección debe ser igual tanto en supuestos de acceso local como remoto (art. 85 RLOPD).

En cualquier caso y sin profundizar mucho más en este apartado técnico, se trata de que una vez determinado este marco de seguridad las normas creadoras de las bases de datos en materia de salud, y la historia clínica digital se encuentra en este ámbito, creen los recursos necesarios para cubrir esta exigencias. En general es una labor de diseñar un sistema que responda a su utilidad y a la vez defina unos objetivos de seguridad proponiendo los medios para conseguirlo.

Así la Ley 3/2005 señala que cada centro sanitario archivará la historia clínica de sus pacientes, cualquiera que sea el soporte (...) 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, así como la autenticidad del contenido de las mismas y su plena reproductibilidad futura*. En cualquier caso, debe garantizarse que queden registrados todos los cambios e identificados los médicos y los profesionales asistenciales que los han realizado.

Igualmente señala que serán los centros sanitarios los que deben adoptar las medidas técnicas y organizativas adecuadas para *proteger los datos personales recogidos y evitar su destrucción o su pérdida accidental, y también el acceso, alteración, comunicación o cualquier otro procesamiento que no sean autorizados*.

Igualmente se desarrollan en el art. 33 de la Ley 3/2005 los detalles de utilización de la Historia Clínica lo que en suma determina un desarrollo de niveles de usuarios y perfiles que garantizaran los accesos exclusivos y adaptados a cada función.

La tabla siguiente³ muestra de forma conjunta los objetivos de seguridad y las medidas o mecanismos de seguridad que existen para garantizar su cumplimiento.

³ Adaptado de "La seguridad, confidencialidad y disponibilidad de la información clínica", Informes Sociedad española de Informática de la Salud, 2003, citada, pág. 259

OBJETIVOS	DESCRIPCIÓN	MEDIDAS
Identificación de usuarios	Es el proceso de identificar al cliente de la aplicación o servicio. No olvidar que los clientes pueden ser tanto personas, como otros servicios, procesos y otros ordenadores	Certificados digitales
Confidencialidad de contenidos	Consiste en asegurar que a la información solo accede quien está autorizado para ello.	Cifrado, encriptación
Integridad de los datos	Conjunto de acciones que garantizan que la información no se ha transformado durante su procesado, transporte o almacenamiento.	Firma digital
No repudio	Procedimientos para asegurar que ninguna de las, partes implicadas ya identificadas (autenticadas) puede negar haber participado en una determinada transacción.	Firma digital, auditoria.
Autorización individualizada	Determinar a qué información puede acceder y qué tareas puede acometer, un cliente autenticado, por lo tanto identificado con certeza Este proceso determina los privilegios asociados a un perfil de usuario	Cuestión organizativa que debe diseñar cada organización y llevar a cabo en sus sistemas particulares.
Auditoria	Es la posibilidad de poder rastrear los accesos realizados a la información y las operaciones hechas sobre ella por cada usuario y las circunstancias en que las hizo.	Registros de acceso y operaciones efectuadas sobre la información
Disponibilidad de los contenidos	Forma parte de la seguridad el poder disponer de la información cuando se necesite. Por ello se deben proteger los sistemas de forma que se mantengan en funcionamiento y se pueda acceder a la información en cualquier momento	Operación y nivel de servicio adecuados sobre los sistemas

Partiendo de la base de que los dos mecanismos básicos de seguridad son las *claves públicas y privadas*, y *los algoritmos de resumen de una dirección*. Estos son los fundamentos para la construcción del resto de mecanismos de seguridad. Mediante la combinación de todos ellos se consigue proteger los sistemas de información mediante el *cifrado o encriptación*, *la firma* y *los certificados digitales*. Estos son los mecanismos técnicos de protección de la información. Los mecanismos básicos y técnicos se complementan con los de *organización de autorización y auditoria*, así como con los de *operación y de nivel de servicio*.

3.- SISTEMAS DE SEGURIDAD USADOS HABITUALMENTE

Tanto en el ámbito privado como en el de la administración pública es cada vez más extendido el uso de sistemas de seguridad para almacenar y transmitir la información necesaria para desempeñar las funciones propias de cada sector. Si bien, como ya podemos suponer, no existe ninguna forma de eliminar totalmente los riesgos asociados a la utilización de los sistemas de historias clínicas informatizadas, especialmente en un entorno de redes, los centros sanitarios han tomado una serie de medidas para garantizar la seguridad de los datos y prevenir el mal uso de la información o los errores en las historias clínicas informatizadas.

Existen una serie de sistemas de seguridad a los que ya hemos aludido en la tabla anterior que son los más usados, aunque no siempre bien y no siempre todos. Como el propósito de este trabajo no es formar técnicamente sino informar del estado de la cuestión, los enumeraré y describiré brevemente.

Claves públicas y privadas

Son mecanismos básicos de seguridad. Consisten en la *generación* mediante algoritmos matemáticos u otros dispositivos o técnicas, *de pares de claves*, cada uno de los cuales está compuesto por la clave privada, conocida solamente por el propietario del par de claves, y la clave pública, que el propietario puede enviar a quien desee para que pueda disponer de la información encriptada.

Estos pares de claves tienen las siguientes características:

- Están relacionadas entre sí de forma especial pues la correspondencia entre ellas es única.
- No se puede nunca deducir una a partir de la otra.

- La clave privada solo es conocida por su propietario y nunca se debe compartir como medida de seguridad.
- La clave pública se distribuye por el titular y puede ser conocida por cualquiera que intervenga en una operación en la que se utilice estos mecanismos.

Algoritmos de resumen de una dirección

Mediante un algoritmo matemático (hash), a partir de una determinada información se genera un resumen de los datos representado por una secuencia de letras y números incomprensible, “aparentemente” aleatoria, ya que para cada documento o grupo de datos existe uno y no puede coincidir con otro.

Este resumen o HASH tiene dos características:

- Es imposible, usando procesos inversos o de cualquier tipo, que se pueda obtener el original de los datos a partir del resumen.
- Es único, ya que a partir de unos datos determinados siempre se obtiene un resumen y solo ese resumen, y cualquier alteración mínima de los datos genera un HASH diferente.

Es ampliamente utilizado a nivel internacional y sirve eficazmente para la identificación absoluta de archivos en todo tipo de investigaciones, llegando a ser considerado como la huella digital de los delitos informáticos, de forma que garantiza que el archivo obtenido en la investigación es el mismo que se recogió y no ha sido alterado en el proceso de análisis.

Cifrado o encriptación

El cifrado o encriptación consiste en la *transformación de una información de manera que solamente la entiendan el emisor y el receptor*. Este se puede aplicar a cualquier tipo de información, como documentos, correo y formularios electrónicos entre otros y provoca que el sujeto ajeno a la comunicación que accede al documento observa algo absolutamente incomprensible e incluso diferente a lo que realmente representa.

Cifrado privado

El cifrado privado es el que se *utiliza para la firma digital común*. En este proceso se encripta la información de forma que cualquiera que la reciba sea capaz de entenderla, pero lo que se asegura es que el emisor de la información es quien dice ser.

Cifrado público

El cifrado público es el *cifrado clásico utilizado para enviar información cifrada* entre dos extremos de forma que solamente estos extremos son capaces de entenderla. En este proceso se encripta la información para un destinatario concreto, asegurando que solo él podrá comprenderla. Lo que se asegura es que solo un destinatario, y exclusivamente ese destinatario, recibirá el mensaje de forma correcta.

Firma digital

La utilización de historias clínicas informatizadas obliga a que los facultativos u otro personal responsable de la atención del paciente deban autenticarse, es decir, certificar quién efectúa la introducción de datos en el sistema informático.

Mediante el mecanismo de firma digital, mediante el uso de tarjetas criptográficas o similares, no solo se asegura la *autenticidad de la identidad del emisor de la información*, si no que se asegura también que los *datos no han sido manipulados durante el envío*.

El proceso necesario para realizar la firma digital de una información es el siguiente:

1. Se obtiene un resumen de los datos a firmar mediante un algoritmo hash.
2. Este resumen se encripta con la clave privada del emisor mediante un algoritmo de clave pública. Al producto de la encriptación del resumen se le llama la firma digital del documento.
3. Esta firma digital se adjunta al documento original de forma que cualquiera pueda comprobar su autenticidad.

Solo el emisor conoce su clave, es el sistema que todos conocemos de tarjeta criptográfica que requiere un pin cada vez que interactuamos con el sistema y que para que sea seguro realmente obliga al titular a ser respetuosos con las limitaciones y recomendaciones de seguridad⁴.

⁴ Ver las recomendaciones de la American Health Information Management Association (AHIMA) acerca del uso de las firmas electrónicas.

Certificado digital

El certificado digital es el mecanismo independiente que *permite garantizar que una clave pública enviada por un interlocutor es verdadera*. El certificado digital contiene todos los datos que el usuario expone al exterior y que permite comprobar que la clave pública es válida y es además de quien dice ser.

El contenido mínimo de un certificado consiste en los siguientes elementos:

- Datos de identificación del titular del certificado.
- Clave pública del titular.
- Datos de la autoridad de certificación que lo emitió.
- Fechas de expedición y expiración de la validez del certificado.
- Usos para los que está autorizado este certificado.
- Número de serie.
- Algoritmo de encriptación utilizado para firmar.
- Firma digital de la autoridad certificadora (firma del resto del contenido del certificado de forma que se pueda consultar su validez).

Mecanismos organizativos de autorización y auditoría

Asignación de perfiles y roles

Antes de implantar un sistema de información clínico se debe *definir quién puede acceder a qué contenidos de la información y qué acciones se pueden llevar a cabo sobre ella*. Es decir, se debe establecer qué perfiles de usuario se desea que existan para el sistema, indicando a qué nivel de información pueden acceder cada uno de estos perfiles, qué operaciones o roles pueden realizar sobre esta información y en qué medida pueden ejercer estos roles, así como durante cuánto tiempo o desde cuándo.

Auditoría

Con independencia de con qué perfil se acceda y las acciones que se lleven a cabo, se establecerán, necesariamente por exigencia legal, los mecanismos que *permitan registrar y dejar un rastro de todas las operaciones que se han hecho con la información*. Se registrará toda la información necesaria para que luego se puedan hacer

auditorías, en las que se determine si el acceso a la información estaba o no justificado, cuando se accedió, como, a que y si se produjo alguna descarga.

En consecuencia, para cualquier acceso, el sistema debería guardar para su uso posterior y consulta⁵:

- Certificación de la identidad del usuario y nivel de autorización.
- Registro de la fecha, hora y ubicación del acceso.
- Registro del tipo de acceso (consulta, creación, modificación o copia).
- Registro del campo o ámbito de acceso.

Mecanismos de disponibilidad

Además de garantizar la confidencialidad e integridad de la información sanitaria, se hace necesario que esté *accesible para las personas autorizadas y que éstas puedan llevar a cabo sus transacciones cuando lo necesiten*. Las catástrofes en materia de protección de datos no siempre son por accesos indebidos o por pérdida de la información, también lo son por no poder acceder, disponer, de la información cuando ésta es necesaria, por ejemplo al no estar debidamente indexada o erróneamente clasificada.

El diseño correcto de estos mecanismos debe garantizar siempre el nivel de seguridad alto especificado para los datos relativos a la salud (LOPD) y reunir una serie de requisitos exigidos por la norma, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (Art. 104 RLOPD).

Plan de recuperación de la información ante catástrofes

Además, de la realización de copias de seguridad y el almacenamiento externo de forma regular de todos los datos de valor, se debe contar con un plan de prevención que permita la recuperación de la información en caso de catástrofe de cualquier

⁵ La seguridad de la información en las historias clínicas informatizadas”, J. Renau Tomás, I. Pérez Salinas, Unidad de Documentación Clínico y Admisión. Hospital General de Castellón. Papeles Médicos 2000; 9 (1); 49, pág. 6.

tipo que pudiera provocar la pérdida o inutilización de los datos y las consecuencias de esto en el servicio prestado.

Las normas de seguridad exigen siempre que la información sanitaria se halle protegida contra pérdidas, destrucción, manipulación, y acceso o uso por parte de personal no autorizado.

Correcta destrucción de los datos

En aquellos casos, casi todos, en los que dentro de la política de conservación documental se prevea y se realice la destrucción de determinados datos informatizados de las historias clínicas hay que obrar con mucha cautela. Además de borrar los datos almacenados en soporte magnético se destruirán también todas las copias de seguridad, así como las copias remotas creadas en un sistema de red sanitaria. Se debe garantizar que la confidencialidad se halla preservada incluso durante el proceso de destrucción de datos.

4.- LA DISUASIÓN.

Como ya he mencionado hay un nivel más de seguridad que tiene como misión la disuasión ante comportamiento de ataque a la seguridad de los datos recogidos en los sistemas informáticos de los sistemas de salud.

En un primer escalón están los controles específicos de cumplimiento de las reglas de creación y gestión de las bases de datos, recogidos en la LOPD y en su Reglamento.

El Régimen sancionador se regula en los arts. 120 a 129 RLOPD que diseñan el sistema de actuaciones previas y de inicio del proceso sancionador, que determinan la existencia o no de infracción.

Por su parte la ley establece un catálogo de infracciones (art. 44 LOPD), graduadas en leves, graves y muy graves, en una lista cerrada.

A cada tipo de infracción le corresponde una sanción de las descritas en el catálogo de sanciones (art. 45 LOPD), regulándose la graduación de estas y la posible sustitución de las mismas por obligaciones de corrección de las deficiencias advertidas.

Cuando se trata de administraciones públicas, además de los requerimientos oportunos, cabe la posibilidad de sanciones disciplinarias en el ámbito del derecho administrativo sancionador de funcionarios públicos, como responsables de las conductas objeto de expediente.

Ejemplos de expediente sancionadores de la Agencia de Protección de Datos son:

1. Procedimiento número AP/00059/2015, RESOLUCIÓN R/00814/2016 de la APD contra el Instituto Nacional de Toxicología y Ciencias Forenses, donde se examinan diversas infracciones que conducen a la falta de seguridad exigible a un sistema concreto de nivel alto de protección.
2. Procedimiento número AP/00061/2015, RESOLUCIÓN R/00711/2016 de la APD contra el CENTRO PENITENCIARIO de SEVILLA, (Secretaría General de Instituciones Penitenciarias), por irregularidades en la gestión y acceso del fichero sanitario del citado centro.
3. Procedimiento número AP/00045/2015, RESOLUCIÓN R/03405/2015 de la APD contra la entidad SERVICIO DE SALUD DE CASTILLA LA MANCHA (SESCAM), por divulgación de datos de pacientes incluidos en la HCD (número y planta de la habitación del paciente y necesidad concreta de prótesis)

Un segundo nivel de disuasión, ya más grave, es el ámbito penal del que solo mencionaré algunas cuestiones puntuales, dado que ya se ha hablado sobre ello, con ejemplos.

DELITOS CONTRA LA INTIMIDAD (arts. 197 a 201 del CP)

La autoría de estos delitos no está reservada solamente al personal no autorizado, terceros ajenos a los servicios, sino a aquel que excede la autorización que posee y accede a datos que no necesita conocer por su labor profesional.

Y así en la STS de 6-10-2015⁶, El TS *considera que la actuación voluntaria de un Magistrado de acceder al Registro de penados, al margen de cualquier procedimiento, podría ser constitutivo indiciariamente de un delito de descubrimiento y revelación de secretos*”.

Por su parte en la STS 3-2-2016⁷, se señala que *“las distintas modalidades de acción implican una agresión a la custodia de los datos que aparece expresada con el término “sin estar autorizado” lo que implica no sólo un acceso no permitido a la información reservada, como el que pudiera realizar una persona ajena a la base de datos o al archivo que incluye los datos especialmente protegidos, también un acceso realizado por un autorizado fuera del ámbito de la autorización”*.

⁶ STS Sala 2ª de 6 octubre 2015, (datos reservados, autoría Art. 197-2), EDJ 2015/173675.

⁷ STS Sala 2ª de 3 febrero 2016, (acceso a datos, Art. 197-2), EDJ 2016/2977.

Solo basta el mero acceso a los datos AAP Cantabria 25-11-2015⁸, ya que *“la historia clínica definida en el artículo 3 de la Ley 41/2002, como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, estaría comprendida en ese derecho a la intimidad y además forma parte de los datos sensibles, esto es de aquellos pertenecientes al núcleo duro de la privacidad, cuyo mero acceso, como hemos descrito, determina y lleva implícito el perjuicio de tercero exigido en el tipo penal”*;

DAÑOS INFORMÁTICOS. (arts. 263 a 264 ter del CP)

El *objeto* de estos delitos son los datos, sistemas o programas informáticos y documentos electrónicos ajenos.

Las conductas típicas son borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles estos datos o documentos o bien obstaculizar o interrumpir funcionamiento de un sistema informático con resultado grave.

La SAP Madrid de 23-10-2015⁹, insiste en la necesidad de que el daño causado se pueda considerar grave, y aporta unos breves criterios de referencia, para que haya delito.

Por su parte la SAP Madrid de 8-2-2016¹⁰, señala que el delito de daños informáticos conlleva casi necesariamente el acceso no autorizado al sistema informático que alberga los datos o documentos atacados, accesos que debe calificarse de ilícito.

A MODO DE CONCLUSIÓN

En este punto asumo íntegramente, adaptándolo a la actualidad, lo que ya se dijo en el trabajo de J. Renau Tomás y I. Pérez Salinas¹¹, la tecnología en la gestión de la atención sanitaria es ya una realidad. La industria de atención sanitaria está bajo una continua presión para reducir costes sin reducir la calidad y cantidad de los ser-

⁸ AAP Cantabria de 25 noviembre 2015, (acceso a fichas de datos Historia Clínica Digital), EDJ 2015/269468.

⁹ SAP Madrid de 23 octubre 2015, (necesidad de resultado e intromisión grave), EDJ 2015/208788.

¹⁰ SAP Madrid de 8 febrero 2016, (daños a sistemas y acceso no autorizado), EDJ 2016/16709.

¹¹ La seguridad de la información en las historias clínicas informatizadas”, J. Renau Tomás, I. Pérez Salinas, Unidad de Documentación Clínico y Admisión. Hospital General de Castellón. Papeles Médicos 2000; 9 (1); 49, pág. 9.

vicios sanitarios prestados y un método eficaz para lograrlo es llevar a cabo redes de información sanitaria. La informatización a gran escala mediante redes de transmisión de datos sobre atención sanitaria disminuye los costes de obtención de datos y minimiza el tiempo de búsqueda. Asimismo, la tecnología de redes se adapta al cambio que se viene produciendo en el mundo de la atención sanitaria, en el que la cantidad de información en constante aumento únicamente es igualado por la necesidad de recuperarla de forma rápida y eficaz.

En este marco un aspecto clave en el diseño de los sistemas de historias clínicas informatizadas es el de garantizar la seguridad de los datos del paciente. La seguridad total es inalcanzable, pero en la actualidad existen medios técnicos que permiten obtener niveles aceptables de seguridad en la gestión de los datos considerados sensibles. Creo que desdeñar su uso o ahorrar costes en esta materia es un error, y los errores en esta materia se pagan caros.

BIBLIOGRAFÍA CONSULTADA

- “La seguridad, confidencialidad y disponibilidad de la información clínica”, José Antonio Garbayo Sánchez, Jokin Sanz Ureta, Javier Carnicero Giménez de Azcárate, Carlos Sánchez García, Informes Sociedad española de Informática de la Salud, 2003, págs. 256-286.
- “El sistema de historia clínica digital del Servicio Nacional de Salud”, Instituto de Información Sanitaria, Agencia de Calidad del Sistema Nacional de Salud, NIPO en línea: 840-09-110-6.
- “La seguridad de la información en las historias clínicas informatizadas”, J. Renau Tomás, I. Pérez Salinas, Unidad de Documentación Clínico y Admisión. Hospital General de Castellón. Papeles Médicos 2000; 9 (1); 49
- “Manual de salud electrónica para directivos de servicios y sistemas de salud”, Publicación de las Naciones Unidas, 2012.
- “Historia Clínica Electrónica. Jara Asistencial: Mirada desde la Seguridad”, Ángel Paredes Menea. Presentación, AEGRIS, XI Congreso, 2008
- “La explotación de datos de salud. Retos, oportunidades y límites”, Alberto Andérez González, Juan Díaz García, Fernando Escolar Castellón, Pilar León Sanz, Sociedad española de Informática de la Salud. 2016.
- “Proyecto Jara, sistema integrado sistema de información sanitaria”, Francisco Manuel García Peña, Director Gerente del Servicio Extremeño de Salud. <http://www.fgcasal.org/medicinaenred2/Garcia.PDF>

RESOLUCIONES DE LA AEPD.

- AAPP-00045-2015. Resolución de 3-01-2016, aplicación del artículo 10 LOPD
- AAPP-00059-2015. Resolución de 20-04-2016, aplicación del artículo 9 LOPD
- AAPP-00061-2015. Resolución de 18-04-2016, aplicación del artículo 9 LOPD

JURISPRUDENCIA.

- STS Sala 2ª de 6 octubre 2015, (datos reservados, autoría Art. 197-2), EDJ 2015/173675.
- SAP Madrid de 23 octubre 2015, (necesidad de resultado e intromisión grave), EDJ 2015/208788.
- AAP Cantabria de 25 noviembre 2015, (acceso a fichas de datos Historia Clínica Digital), EDJ 2015/269468.
- STS Sala 2ª de 3 febrero 2016, (acceso a datos, Art. 197-2), EDJ 2016/2977
- SAP Madrid de 8 febrero 2016, (daños a sistemas y acceso no autorizado), EDJ 2016/16709.

**PROBLEMÁTICA DE
LA CONFIDENCIALIDAD EN
LOS DIFERENTES MEDIOS
DE LA MEDICINA**

**PROBLEMÁTICA DE LA CONFIDENCIALIDAD
EN LOS DIFERENTES MEDIOS DE LA MEDICINA:
EN ATENCIÓN PRIMARIA**

Félix Suárez González

Médico de Familia. Centro de Salud San Roque. (Badajoz).

1.- CONFIDENCIALIDAD EN ATENCIÓN PRIMARIA SUS PROBLEMAS PROBLEMAS QUE SUBYACEN EN LA CONFIDENCIALIDAD

La confidencialidad en medicina es obligatoria, como no puede ser de otro modo, y podemos nombrar desde la intimidad, privacidad, confianza, fidelidad y lealtad que existe en la relación clínica y en la atención sanitaria; las obligaciones de confidencialidad, secreto, sigilo o reserva para los profesionales; la información a terceros, con su justificación y límites, el deber de tratar, deber de alertar, la posición de garante, así como el estado de necesidad.

También tenemos que considerar los límites a la obligación de confidencialidad. Qué revelación es permisible y qué revelación se exige; también el efecto del tipo de peligro o daño al que se exponen terceros.

Es importante ver la actitud del profesional sanitario ante la confidencialidad en la propia institución sanitaria, la confidencialidad y trabajo en equipo, la elaboración, registro, almacenamiento, informatización y acceso a la historia clínica.

2.- ASPECTOS ÉTICOS DE LA RELACIÓN CLÍNICO-ASISTENCIAL

En primer lugar, resulta necesario discernir entre privacidad y confidencialidad, ya que los profesionales conocen datos íntimos de los pacientes que no son relevantes en muchos de los casos para la asistencia.

Por otra parte, el médico debe saber informar guardando el secreto profesional, de forma que la información que se comparta con el equipo sanitario, familiares, conocidos o extraños proteja la privacidad del paciente.

Es necesario identificar y corregir los prejuicios que puedan tener los profesionales, así como la actitud del médico según sus valores morales y religiosos y los del paciente.

También se debe tener en cuenta la dificultad que surge para establecer límites en la relación clínica y hasta dónde interfieren en el estilo de vida de los pacientes y sus familias.

3.- CONFIDENCIALIDAD EN LA HISTORIA CLÍNICA DIGITAL

Debemos tener en cuenta la Integridad: que asegura que la información contenida en el texto electrónico no ha sido modificada luego de su firma, la Autenticación: que es la información del documento y su firma que se corresponden con la persona que

ha firmado. No se debe Mentir, ya que la persona que ha firmado no puede decir que no lo ha hecho; y por último la Confidencialidad: que es la información contenida que ha sido cifrada y la voluntad del emisor, que solo permite que el receptor que él determine pueda descifrarla.

3.1 VENTAJAS DE LA HC DIGITAL

No cabe duda que ha sido una ayuda al profesional en su práctica clínica diaria, sobre todo, hasta ahora en las ayudas a la prescripción farmacéutica y a la codificación, la facilitación, y la ordenación, que disminuye progresivamente el espacio necesario para su almacenamiento. Sirve de instrumento de ayuda para la investigación y la docencia mediante el fácil acceso a datos estadísticos y fuentes bibliográficas. Facilita el acercamiento entre la tarea asistencial y la de gestión. Es más segura y facilita la confidencialidad de los datos para el paciente.

3.2 DESVENTAJAS DE LA HC DIGITAL

Entre otras, la posible resistencia a utilizar una metodología distinta que obliga a estudiar cosas nuevas: los diferentes modelos de las distintas comunidades autónomas, ya que es muy lento y engorroso cargar los datos. Hay que ingresar muchos datos para cada paciente. Hay que invertir dinero en equipamiento, y personal informático, si se quiere ser eficiente, por lo que si no existe una metodología adecuada al cargar los datos, las búsquedas son inexactas

4. PROCEDIMIENTO DE ANÁLISIS DE CONFLICTOS ÉTICOS

Para analizar si existe un conflicto ético, primero tenemos que presentar el “caso” objeto de análisis; después hay que aclarar los “hechos” propios del caso (tanto datos objetivos como subjetivos); identificar los “valores” en conflicto en el caso; analizar los “cursos de acción” posibles

- Identificar los “cursos óptimos; comparando con el marco “jurídico” pertinente al caso

4.1 PROBLEMAS FRECUENTES EN ATENCIÓN PRIMARIA

4.1.1 Conflictos entre el secreto profesional y el deber de protección de la vida de terceros; esto, a su vez se fundamenta en la relación de confianza entre el médico y el paciente, fundamental para la consecución de los objetivos de la relación clínica.

De una parte, la protección de la vida de una o varias personas, y el derecho de los pacientes a la confidencialidad de sus datos y obligación de secreto de los profesionales.

De otra, el derecho que el paciente tiene al respeto de su intimidad y confidencialidad de sus datos, y el deber correlativo del profesional a respetarlos.

4.1.2 Cuando hay actuación de los profesionales en procesos judiciales en calidad de peritos o testigos, es imprescindible el deber de colaborar con la Justicia, que puede constituirse en una auténtica obligación o deber inexcusable si el Juez instructor obligara al médico a elaborar el informe pericial o a prestar declaración. Así tenemos de una parte, el del secreto profesional del médico, y de otra parte la garantía de los intereses públicos que siempre conlleva la persecución de una actividad criminal.

En el supuesto de que se exija al médico acudir como perito, debería formalizar un escrito fundado y presentarlo ante el propio Juzgado, con indicación de las circunstancias que impiden emitir el informe pericial, desde dos aspectos: el del secreto profesional y el de las razones de la abstención, por haber tenido el paciente una relación directa de dependencia con el profesional.

En el caso de que el médico sea citado para acudir como testigo, ante todo debe comunicar que tiene el deber de guardar secreto sobre todo aquello que guarde una estrecha relación con el tratamiento y los datos internos que se hayan obtenido de la relación profesional con el paciente investigado. En caso de que el Juez no le libere de responder a alguna de las preguntas intimidad, confidencialidad y secreto, el médico debe advertir en cada una de sus respuestas que entiende está sujeto al deber de secreto profesional y que con el caso concreto que se plantea, o exponer opiniones personales sobre su paciente. contesta por imponerlo el Juez. Asimismo, el médico debe centrarse en el contexto de la propia pregunta y evitar supuestos hipotéticos o extremadamente subjetivos, o aquellos que ninguna relación guarden.

4.1.3 El conflicto entre el secreto profesional y el uso de la información clínica por otros profesionales sanitarios o no sanitarios. La información no puede utilizarse con una finalidad distinta de aquella para la que fue recopilada y para la que el paciente dio su permiso.

4.1.4. El conflicto entre accesibilidad y protección de la historia clínica

La historia clínica tiene como fin principal facilitar la asistencia sanitaria; es un instrumento destinado a garantizar una asistencia adecuada al paciente, razón por la cual comprenderá el conjunto de documentos relativos a los procesos asistenciales de que sea objeto, incorporando la información que se considere trascendental para

el conocimiento veraz y actualizado del estado de su salud. Pero, además, la historia clínica es la fuente de información necesaria para otros muchos fines para los que debe ser útil, entre los que se enumeran los judiciales, epidemiológicos, de salud pública, de investigación o de docencia, todos ellos legítimos y constitutivos de actuaciones fundamentales del Sistema Sanitario. Los valores implicados son el derecho a la información de los familiares del paciente, el derecho del paciente a la confidencialidad y el derecho del médico a la reserva de sus anotaciones subjetivas. Debe controlarse quién está utilizando la historia desde su salida del fichero hasta su devolución.

4.1.5 El conflicto del médico que entra en conocimiento de datos confidenciales.

La confidencialidad de los datos es un valor importante. Pero también es un valor la protección de la salud de las personas en riesgos de sufrir agresiones que pueden llegar a ser mortales.

El análisis ético no debe confundirse con el análisis legal de los problemas. Algo puede ser éticamente malo y legalmente correcto, y viceversa. No es bueno resolver el problema apelando simplemente a la ley y revelando la situación del paciente. Es preciso hacer todo lo posible por salvar los dos valores en conflicto. Todos tenemos la tendencia a convertir los problemas en dilemas, y por tanto a pensar que la cuestión no tiene más que dos salidas posibles. Eso suele deberse a pereza mental. Todo problema suele tener más de dos cursos de acción posibles. Y como regla general cabe decir que los cursos extremos, que son los que primero y con mayor claridad se ven, son también los más lesivos. Los cursos óptimos suelen ser los intermedios.

4.1.6. El conocimiento de negligencias profesionales

La mejor protección contra las denuncias de los pacientes es una buena relación clínica, basada en la sinceridad, la objetividad y la confianza. Cuando existe Intimidad, confidencialidad y secreto, la relación clínica es buena, las denuncias son infrecuentes, incluso en casos flagrantes de negligencia; por el contrario, cuando la relación es mala, las denuncias se multiplican, incluso sin causa objetiva para ello. La promoción de la calidad ética en las instituciones es la mejor garantía para éstas y para sus profesionales.

4.1.7. La situación particular de los estudiantes de medicina.

No puede revelarse nada que tenga relación con la vida, salud, enfermedad o sexualidad de las personas, sin su expreso consentimiento o sin que una norma lo habilite. El secreto compartido obliga a todas las personas que, por su profesión, se

ven involucradas en la asistencia al enfermo: médicos consultores, ayudantes, residentes, diplomados en enfermería, matronas, etc.

4.1.8. El exceso de locuacidad del personal sanitario

Como en todos los casos previos, uno de los valores implicados es la necesaria confidencialidad de todos los datos sanitarios. La ruptura de la confidencialidad se hace con frecuencia por motivos completamente injustificables. En esos casos no es posible hallar otro valor positivo que pueda contraponerse al de la confidencialidad. Pero en otras ocasiones, sí pueden encontrarse valores positivos. Así, los profesionales comparten la información para contrastar sus decisiones clínicas y asegurar la buena asistencia del paciente. Respecto a los comentarios sobre la salud de los pacientes realizados en pasillos, ascensores o cafetería, hay que tener en cuenta que el hecho de que el interlocutor sea médico o enfermero no libera de la obligación de sigilo. Mucho más cuidado hay que tener con cualquier comentario con amigos sobre el estado de salud de una persona identificable. El deber de secreto médico alcanza no sólo a los aspectos estrictamente médicos, sino también a los que se puedan conocer o intuir de otras muchas facetas de la vida del paciente o de terceros con quienes aquél se relaciona, y que se hayan conocido durante el acto médico.

4.1.9. Comentarios personales y acceso a la propia historia clínica.

Ante la petición del paciente, el profesional se encuentra en la necesidad de atender a dos valores en muy buena medida contrapuestos. De una parte, el derecho del paciente a la información sobre su cuerpo y su salud, y más en concreto a la historia clínica.

Cuando el paciente solicita del médico de cabecera que se le entregue la historia clínica, éste debe informarle de los límites que tiene en relación a dicha historia y que se establecen en nuestro ordenamiento jurídico: la confidencialidad de las terceras personas cuyos datos constan en la historia clínica y las anotaciones subjetivas que el propio médico ha apuntado. Junto a la referida información, el médico de familia entregará al paciente una copia autenticada de la historia sin aquellos datos protegidos, salvo que le otorguen consentimiento las personas que se citan en la historia clínica, en cuyo caso también le entregará los datos relativos a ellas.

Se intentarán establecer los mecanismos de custodia que eviten que el paciente tenga libre acceso a la historia clínica, y que impidan también el acceso de terceros ajenos al tratamiento. La historia se redactará y elaborará de forma comprensible,

con criterios unificados dentro del Centro de Salud y en lo posible a través de un método que disocie los datos clínicos del paciente de los de terceras personas ajenas al tratamiento y de las anotaciones subjetivas de los médicos.. La historia clínica tiene como finalidad permitir un conocimiento veraz y actualizado del estado de salud del paciente, posibilitando la identificación de los médicos y de los demás profesionales sanitarios que intervienen en los procesos asistenciales. Se debe proteger adecuadamente datos que se consideran especialmente sensibles y por tanto, necesitados de la custodia más rigurosa posible.

4.1.10. El acceso a la documentación clínica, sin consentimiento expreso de los pacientes, por parte de los administrativos y el personal laboral.

Es exigible que un centro sanitario cumpla con las normas legislativas en materia de confidencialidad de datos clínicos. En caso de detectar dificultades para el cumplimiento de estas normas, debe denunciarse por escrito ante la dirección del centro, ya que de lo contrario se compartiría la responsabilidad de posibles conflictos. b) Ante cualquier problema que pudiera atentar al derecho de confidencialidad de los pacientes, el médico debe extremar las salvaguardas y, a la vez, denunciar todo defecto advertido en la adecuada protección de los datos. Tanto los médicos que ejercen en atención primaria de salud como en hospitales, deben pedir a sus organizaciones representativas que insten a la Administración para que solucione los problemas relativos a la confidencialidad de los datos clínicos.

5. CONCLUSIONES

- a) Registrar informáticamente la historia clínica de los casos más problemáticos con algún código de seguridad que impida su acceso independiente a todos los profesionales no directamente implicados en la asistencia del caso (enfermeras, secretarías, u otros médicos)
- b) Implantar algún sistema de seguridad en la tramitación, almacenaje y recepción de volantes comprometedores para personas determinadas.
- c) Asegurar que el registro de los volantes sea realizado por una sola persona responsable e identificable.
- d) Marcar con alguna señal los volantes que se quiera mantener ocultos.
- e) Disponer de un lugar de acceso restringido para almacenar los volantes marcados,

o portadores de datos particularmente sensibles.

- f) Establecer un sistema de envío de ciertos informes en sobre cerrado, que sólo pueda abrir el médico en cuestión.
- g) Realizar periódicamente actividades de concienciación y recuerdo a todo el personal sanitario de sus obligaciones de confidencialidad (mediante circulación de documentos, reuniones, sesiones, congresos...).

BIBLIOGRAFIA

1. Derecho internacional

Convenio del Consejo de Europa para la protección de los Derechos Humanos y la Dignidad del Ser Humano con respecto a las aplicaciones de la Biología y la Medicina, de 4 de abril de 1997. Entrada en vigor en España: 1 de enero de 2000. Artículo 10

2. Derecho comunitario

Directiva 95/46/CE, sobre la protección de las personas físicas respecto al tratamiento de datos personales y la libre circulación (trasposición mediante la Ley Orgánica de Protección de datos, Ley Orgánica 15/1999, de 13 de diciembre)

3. Recomendaciones del Consejo de Europa (no vinculantes jurídicamente) (se pueden consultar en <http://www.coe.fr>)

4. Constitución Española, artículos 18.1, 24 y 43

5. Derecho Penal Ley de Enjuiciamiento Criminal: artículos 30, 262 y 259 Código Penal (Ley Orgánica 10/1995, de 23 de noviembre): artículos 197-201, 413-418, 20.5, 20.7 y 450

6. Ley Orgánica 2/1998, de 15 de junio, BOE de 16 de junio de 1998, por la que se modifican el Código Penal y la Ley de Enjuiciamiento Criminal

7. Derecho civil. Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil de los Derechos al Honor, a la Intimidad y la Propia Imagen, artículos 2.1, 2.2, 7.3 y 7.4

8. Derecho internacional Derecho administrativo Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

9. Real Decreto 994/1999 de 1 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal

10. Derecho Administrativo-Sanitario. Ley 14/1986, de 25 de abril, General de Sanidad (art. 10 y 61)

**PROBLEMÁTICA DE LA CONFIDENCIALIDAD
EN LOS DIFERENTES MEDIOS DE LA MEDICINA:
MEDICINA DEL TRABAJO
SALUD LABORAL**

Dr. D. Manuel Fernández Chavero

Especialista en Medicina del Trabajo

SECRETO MEDICO Y SU IMPACTO SOCIAL

Excepciones al deber de Secreto

*No decir más de lo que haga falta,
a quien haga falta y cuando haga falta.*

(André Maurois)

En el Tratado de Medicina del Trabajo del Catedrático de Toxicología D. Fernando Gil Hernández se define el Concepto de Salud Laboral como sigue: *“La Salud Laboral, entendida como sinónimo de prevención de riesgos laborales o salud y seguridad en el trabajo y no de medicina del trabajo, se ocupa de todos los aspectos que intervienen en el binomio trabajo / salud de mutua interdependencia, en donde las condiciones de trabajo claramente influyen en la salud del trabajador y, al mismo tiempo, el trabajo se ve afectado por el nivel de salud de dicho trabajador”.*

La Medicina del Trabajo es una especialidad de orientación social con tres fines bien diferenciados: preventivo, clínico y pericial. La Medicina del Trabajo ha sido definida por la Organización Mundial de la Salud como: *“La especialidad médica que, actuando aislada o comunitariamente, estudia los medios preventivos para conseguir el más alto grado de bienestar físico, psíquico y social de los trabajadores, en relación con la capacidad de éstos, con las características y riesgos de su trabajo, el ambiente laboral y la influencia de éste en su entorno, así como promueve los medios para el diagnóstico, tratamiento, adaptación, rehabilitación y calificación de la patología producida o condicionada por el trabajo”.*

EL Profesor D. Enrique Villanueva, actual Presidente de la Comisión Central de Deontología, tiene desarrollado en el curso de Experto en Ética Médica un capítulo titulado “Profesionales con Lealtades Compartidas” se puede leer textualmente: *“El médico del trabajo es un árbitro que se situará siempre del lado de la razón y la justicia. Su lealtad estará al lado del trabajador cuando el empresario restrinja, obstaculice o intente ocultar situaciones de riesgo o produzca con su consulta una precariedad en las medidas de higiene y seguridad. Su lealtad estará con la empresa cuando el trabajador con su conducta absentista, obstruccionista, imprudente, o de enfermedad cree un peligro material para la empresa y sus operarios o para su viabilidad económica o un fraude para las Mutuas Patronales o la Seguridad Social. El Médico del Trabajo se verá protegido por la ley cuando un empresario pretenda coaccionarlo para tomar medidas contra los trabajadores o pretenda eludir o minimizar las medidas de vigilancia y control que la ley le impone para la protección de la salud del trabajador”.*

Las funciones del Médico del Trabajo son fundamentalmente cinco:

- *Promoción*: Conjunto de actividades cuyo objetivo es mejorar el nivel de salud de los trabajadores mediante intervenciones destinadas a capacitarlos para incrementar el control sobre su salud y mejorarla, tanto frente a los riesgos laborales como extra-laborales.
- *Prevención*: Conjunto de actividades cuyo objetivo es reducir o eliminar riesgos laborales mediante intervenciones colectivas o personales.
- *Vigilancia*: Conjunto de actividades cuyo objetivo es la detección precoz de alteraciones de salud, principalmente relacionados con el trabajo, mediante procedimientos de recogida sistemática y análisis de información tanto a nivel individual como colectivo.
- *Asistencia*: Conjunto de actividades que tienen como objetivo el manejo clínico y laboral de los trabajadores con un problema de salud, principalmente aquel relacionado con las condiciones de trabajo.
- *Pericial*: Conjunto de actividades cuyo objetivo es identificar, cuantificar y valorar secuelas de los daños a la salud relacionados con el trabajo y su impacto sobre la capacidad para trabajar con el fin de compensar social y económicamente al trabajador afectado.

El Secreto Médico es tan viejo como la Medicina. Uno de los pilares del prestigio de la Medicina, y por tanto de los médicos, es la discreción. Un acto médico es un ejercicio donde dos personas van a compartir sentimientos, miedos y confidencias. Todo ello emana de la privacidad e intimidad; es decir de aquello que guardamos en nuestro más profundo interior. Por tanto la confidencialidad se construye a cuenta de perder privacidad. A mayor confidencialidad menos privacidad.

CONCEPTOS Y DEFINICIONES

INTIMIDAD: “Lo más interior y reservado de la persona o grupo familiar”. La intimidad se ha referido tradicionalmente a las creencias religiosas y con la actividad moral de la persona. Hoy abarca dimensiones más amplias que las puramente religiosas o morales

PRIVACIDAD: Tradicionalmente se ha referido a limitar el acceso de otros al cuerpo o la mente de uno mediante el contacto físico o la exposición de pensamientos o de sentimientos.

La privacidad y la confidencialidad son similares en cuanto que ambas son contrarias a la idea de “lo público”: lo que es privado y confidencial no es público. Sin embargo privacidad y confidencialidad no son términos equivalentes, abandonar la privacidad personal es una precondition para establecer la confidencialidad. La privacidad es personal, mientras que la confidencialidad requiere de al menos dos personas.

CONFIDENCIALIDAD: “Lo que se hace o dice en confianza, esto es: con seguridad recíproca entre dos o más personas”. Seguridad de qué: de que cada cual conozca su deber y lo cumpla. La confidencialidad se relaciona con la comunicación de información personal y privada de una persona a otra en la que se espera que el receptor de la información no la exponga a terceras personas.

Si bien el secreto se considera un deber para los médicos, no es hasta el siglo XVIII que dicho deber se traduce en la confidencialidad como derecho de los pacientes, produciéndose un gran acercamiento entre la medicina y el derecho.

CONFIDENTE NECESARIO: Todo aquel que queda justificado para conocer datos confidenciales de un paciente o usuario por ser su colaboración necesaria para asegurar la atención sanitaria y los servicios profesionales que hacen necesario recoger información confidencial

ESTADO DE NECESIDAD: Caracterización jurídica de una determinada situación, recogida en el Código Penal, en la que una persona, para evitar un mal propio o ajeno, lesiona un bien jurídico de otra o infringe un deber siempre que concurran los siguientes requisitos:

- Que el mal causado no sea mayor que el que se trate de evitar.
- Que la situación de necesidad no haya sido provocada intencionadamente por el sujeto.
- Que el necesitado no tenga, por su oficio o cargo, obligación de sacrificarse

SECRETO MÉDICO: Compromiso que adquiere el médico, ante el paciente y la sociedad, de guardar silencio sobre toda información que llegue a conocer sobre el paciente en el curso de su actuación profesional. La palabra secreto hace referencia a “lo que debe mantenerse separado de la vista y del conocimiento de los demás”.

El secreto médico como “deber” viene ya recogido en el Juramento Hipocrático: *“Todo lo que vea y oiga en el ejercicio de mi profesión, y todo lo que supiere acerca de la vida de alguien, si es cosa que no debe ser divulgada, lo callaré y lo guardaré con secreto inviolable”* se observa como ya se entiende que el secreto debe mantenerse pero reconoce también la posibilidad de excepción al deber de secreto (“si la cosa no debe ser divulgada”).

Uno de los pilares básicos de la Vigilancia de la Salud de los trabajadores para la consecución de los objetivos mencionados son los Reconocimientos Médicos Laborales (RML).

Los RML generan información sobre el estado de salud de los trabajadores; información que proviene de la intimidad del trabajador y como tal información íntima debe manejarse.

El Artículo 18 de la Constitución reconoce el derecho a la intimidad como un derecho fundamental pero no absoluto. Es un derecho que puede verse limitado o acotado ante situaciones relevantes. Esto mismo va a ocurrir en las relaciones laborales, en la prevención de riesgos laborales. La Ley de Prevención de Riesgos Laborales (Ley 31 /1995) nos queda bien claro que los RML deben llevarse a cabo *“Con especial atención a la protección de la confidencialidad y el respeto a la intimidad”*. En el Artículo 22.2 se nos dice que el derecho a la intimidad, confidencialidad y dignidad del trabajador actúan como límites de la actividad empresarial.

Los datos recogidos en un RML hay que utilizarlos con un especial sensibilidad porque pueden llegar a lesionar otro derecho fundamental del ser humano: El Derecho al Trabajo; *“un derecho fundamental por el que toda persona tiene derecho al trabajo, a la libre elección del mismo, a condiciones equitativas y satisfactorias, a la protección contra el desempleo, sin discriminación, remuneración digna, protección social y derecho de sindicación”*.

En cuanto a la privacidad el trabajador tiene el derecho de mantener ocultos aquellos datos de su estado de salud que nada tengan que ver con los riesgos inherentes de su actividad laboral. Esto último está acorde con la Ley Orgánica 1 /1982 de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Ya hemos reiterado que los RML generan información de la esfera íntima del trabajador; esta información no puede ser manipulada, divulgada o utilizada sin consentimiento del trabajador. Por otro lado existen RML que, por sus motivaciones especiales, han hecho pronunciarse incluso al Tribunal Constitucional. Así ocurre con aquellos RML que pretenden recabar información sobre datos de especial sensibilidad: consumo de estupefacientes, ciertas enfermedades etc. En estos casos hay que realizarlos con el acuerdo explícito del trabajador. El empresario debe informar al trabajador sobre los motivos y finalidades de las pruebas de deben realizarle porque si las pruebas tuvieran una finalidad distinta a la prevención de riesgos laborales no estarían justificadas. En este sentido cabe mencionar la sentencia del Tribunal Constitucional (196/2004): *“Todo aquello que no resulte previsible, y eso es lo que ocurre,*

tratándose de un reconocimiento médico de vigilancia de la salud en función del riesgo laboral, con las pruebas y datos extraños a esa finalidad como sería averiguar el consumo de estupefacientes”.

La Ley de Prevención de Riesgos Laborales, que es el marco legislativo de la actividad preventiva, en su artículo 22 especifica que 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, respetando siempre el derecho a la intimidad y a la dignidad del trabajador y a la confidencialidad de toda la información relacionada con su estado de salud. Además, la LPRL establece, como norma general, la necesidad del consentimiento voluntario por parte del trabajador para poder llevar a cabo la vigilancia de la salud, *derecho que puede perderse excepcionalmente en determinadas circunstancias, previo informe a los representantes de los trabajadores:*

1-Los reconocimientos son obligatorios cuando sean imprescindibles para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores. Artículo 22 de la LPRL.

Cuando se ha tipificado en el puesto de trabajo el riesgo de enfermedad profesional. Por ejemplo, sordera profesional por exposición al ruido, enfermedades de la piel, exposición a tintes, hepatitis por exposición a agentes biológicos...

Artículo 196 de la Ley General de la Seguridad Social

Todas las empresas que hayan de cubrir puestos de trabajo con riesgo de enfermedades profesionales están obligadas a practicar un reconocimiento médico previo a la admisión de los trabajadores que hayan de ocupar aquellos y a realizar los reconocimientos periódicos que para cada tipo de enfermedad se establezcan en las normas que, al efecto, dictará el Ministerio de Trabajo y Seguridad Social.

2: Los reconocimientos son obligatorios cuando sean imprescindibles para verificar si el estado de salud del trabajador puede constituir un peligro para los demás trabajadores o para otras personas relacionadas con la empresa. Artículo 22 de la LPRL.

- Conductores profesionales de vehículos de motor (Real Decreto del Reglamento General de Conductores)
- Conductores y maquinistas ferroviarios
- Manejo de grúas

- Personal de vuelo
- Trabajadores del mar
- Trabajadores sanitarios que realizan procedimientos invasivos, que pueden predisponer a exposiciones a virus de transmisión sanguínea (virus de la hepatitis B o C, VIH) a terceros
- Trabajos con tenencia y/o uso de armas
- Trabajos en alturas
- Trabajos en espacios confinados
- Trabajos subacuáticos
- Trabajadores con riesgo de silicosis
- Trabajos con Cloruro de Vinilo Monómero
- Trabajos con Agentes citostáticos y/o Agentes anestésicos inhalatorios
- Trabajadores ETT (reconocimientos iniciales)

3: Cuando esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad:

- Riesgos biológicos
- Agentes cancerígenos
- Agentes químicos
- Radiaciones ionizantes
- Amianto
- Ruido

4: Cuando así venga establecido en el convenio colectivo.

Por lo tanto en estos RML de obligada realización aún es más necesario ser escrupulosos con la intimidad del trabajador y con el uso y manipulación de sus datos médicos. No se puede obviar que tras el trabajador existe en muchísimas ocasiones una familia cuyo desarrollo y sustento son dependientes del trabajo y del sueldo.

El art. 10 de la Ley General de Sanidad (Ley 14/1986) dispone que todas las personas tienen derecho al respeto de su personalidad, dignidad humana e intimidad, y a la confidencialidad de toda información relacionada con su proceso. Por su

parte, la Ley de Autonomía del Paciente y de Derechos y Obligaciones en materia de información y documentación clínica (41/2002) establece en su artículo 7 que se debe respetar en todas las personas el carácter confidencial de los datos relacionados con su salud y que nadie puede acceder a ellos si previamente no ha sido autorizado. De esta forma se consigue, por un lado, restringir el acceso a tal información, sólo al alcance de los autorizados, y, por otro lado, imponer el deber de reserva y sigilo profesional.

El artículo 22 de la LPRL se refiere a la confidencialidad de toda la información relacionada con el estado de salud del trabajador. El personal médico queda vinculado por la exigencia de confidencialidad, lo que implica que deberá guardar secreto acerca de los datos que conozca de la salud de la persona, tanto dentro como fuera de la empresa, es decir, también frente a terceros, este deber sólo cederá frente a enfermedades infecto-contagiosas. Así pues, salvo que las pruebas determinen falta de aptitud de la persona para el trabajo, en cuyo caso se admite el levantamiento del secreto, para el resto de los casos hay que defender el derecho del trabajador a la confidencialidad de la información relacionada con la salud.

El Tribunal Constitucional nos dice que el Derecho a la Intimidad y Confidencialidad no es un derecho absoluto sino que puede ceder en determinadas situaciones:

- Ante lo límites que imponga la propia Constitución
- Ante la necesidad de preservar otros derechos o bienes jurídicamente protegibles

MARCO ÉTICO

Analicemos ahora la Confidencialidad y el Secreto Profesional desde los fundamentos éticos en los que se sustenta.

Respeto a la autonomía del paciente:

Muchos autores consideran que el respeto a la autonomía personal es la premisa más importante para fundamentar la salvaguarda de la confidencialidad. El argumento sería que sin confidencialidad no hay privacidad, y sin ella se pierde el control de la propia vida.

Existencia de un pacto implícito en la relación clínica:

Una segunda razón que justifica el deber de secreto es la existencia de un pacto implícito en la relación clínica. Esta promesa tácita de discreción puede entenderse como un au-

téntico contrato según el cual se intercambia información, propiedad del paciente, con la condición de que sea utilizada exclusivamente para su atención sanitaria.

Confianza social en la reserva de la profesión médica:

La tercera razón para justificar la obligación de secreto es la confianza social en la reserva de la profesión médica. Si no existiera el compromiso de los médicos de salvaguardar la confidencialidad, los pacientes no se acercarían a la consulta confiadamente.

Lealtad al paciente:

La lealtad es otro modo de enfocar la fundamentación del deber de secreto. Por ella se espera que el facultativo y sus colaboradores hagan uso de la información sólo para la finalidad para la que fue recogida.

MARCO DEONTOLÓGICO

El Código de Deontología Médica dedica el capítulo V al Secreto Profesional del médico y el artículo 30 a las excepciones al deber de secreto.

Artículo 30

El secreto profesional debe ser la regla. No obstante, el médico podrá revelar el secreto exclusivamente, ante quien tenga que hacerlo, en sus justos límites, con el asesoramiento del Colegio si lo precisara, en los siguientes casos:

- En las enfermedades de declaración obligatoria.
- En las certificaciones de nacimiento y defunción.
- Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo.
- Cuando se vea injustamente perjudicado por mantener el secreto del paciente y éste permita tal situación.
- En caso de malos tratos, especialmente a niños, ancianos y discapacitados psíquicos o actos de agresión sexual.
- Cuando sea llamado por el Colegio a testificar en materia disciplinaria.
- Aunque el paciente lo autorice, el médico procurara siempre mantener el secreto por la importancia que tiene la confianza de la sociedad en la confidencialidad profesional.

- Por imperativo legal:
- En el parte de lesiones, que todo médico viene obligado a enviar al juez cuando asiste a un lesionado.
- Cuando actúe como perito, inspector, médico forense, juez instructor o similar.
- Ante el requerimiento en un proceso judicial por presunto delito, que precise de la aportación del historial médico del paciente, el médico dará a conocer al juez que éticamente está obligado a guardar el secreto profesional y procurará aportar exclusivamente los datos necesarios y ajustados al caso concreto.

Artículo 31

- 1: Los resultados de los exámenes médicos exigidos por la Ley, deben ser explicados a la persona reconocida. Solo se informara a la empresa o institución pertinente respecto a la aptitud laboral o de las limitaciones o riesgos para la asignación del trabajo.
- 2: Los resultados de los exámenes practicados en el marco de la vigilancia de la salud se comunicaran exclusivamente a la persona afectada. No obstante, el médico de un centro de medicina preventiva o de medicina del trabajo debe transmitir cualquier resultado que sea útil para el paciente, con su consentimiento, a su médico responsable.

OBLIGACIONES Y CONSIDERACIONES DESDE LA MEDICINA DEL TRABAJO

- Tenemos la obligación de preservar la intimidad y la confidencialidad de los trabajadores.
- Tenemos la obligación de usar los datos derivados de los RMN con cautela y discreción.
- Los datos de un RML pueden ser mal utilizados por el empresario para despidos o discriminaciones laborales.
- El Derecho al Trabajo es un derecho fundamental.
- Comunicar solo lo imprescindible para permitir y hacer útil la corrección de medidas que favorezcan la salud y seguridad de los trabajadores.
- Expresar la información en términos inocuos.

- Informar al empresario de los resultados en términos genéricos y referidos al grado de aptitud del trabajador.
- En situaciones especialmente peligrosas se informará a la empresa y a la autoridad competente.
- El médico del trabajo solo recabará la información que sea pertinente para la protección de la salud en relación con el trabajo. Cualquier otra información deberá contar con el consentimiento del trabajador.
- Es asimismo infracción muy grave la adscripción de trabajadores a puestos de trabajo cuyas condiciones fuesen incompatibles con sus características personales conocidas cuando de ello se derive un riesgo grave e inminente, así como, en dichas circunstancias, la adscripción a puestos de trabajo de los trabajadores que se encuentren manifiestamente en estados o situaciones transitorias que no respondan a las exigencias psicofísicas de los respectivos puestos de trabajo.
- Prudencia y diligencia en la elaboración de informes y certificados pues son documentos médicos-legales de los que emanan graves responsabilidades.

CONCLUSIONES

1. El secreto médico no es absoluto.
2. El derecho a la intimidad no es absoluto.
3. El derecho a la confidencialidad no es absoluto.
4. Existen circunstancias donde el secreto médico puede y debe obviarse en la Medicina del Trabajo:
 - Enfermedades de Declaración Obligatoria
 - Enfermedades infecto-contagiosas
 - Adicciones del trabajador que supongan un serio riesgo para el mismo, los compañeros, la empresa o terceras personas.
 - Trastornos mentales que supongan un riesgo para el mismo, los compañeros, la empresa o terceras personas.
 - Trastornos que ocasionen discapacidades o minusvalías psicorgánicas. Concepto de Apto con Limitaciones.
 - En Peritaciones y requerimientos judiciales.

Es aconsejable que existieran mecanismos de comunicación entre la medicina asistencial, la medicina del trabajo y los centros de acreditación de capacidades psíquicas que lejos de entenderse como una ruptura de la confidencialidad significara una ampliación del círculo de confidentes necesarios para una correcta asistencia integral al usuario y/o paciente y una mayor protección a la sociedad.

REFERENCIAS LEGISLATIVAS:

A: Normativa sobre Salud Laboral

- <http://www.msssi.gob.es/ciudadanos/saludAmbLaboral/saludLaboral/normativa.htm>
- La Constitución Española
- La Ley General de Sanidad, 14/1986
- La Ley de Prevención de Riesgos Laborales 31/1995
- El Real Decreto Legislativo 5/2000
- El Real Decreto Legislativo 1/1994
- Reglamento de los Servicios de Prevención, R.D. 39/1997
- Orden De 27 De Junio De 1.997
- Acuerdo de Criterios Básicos para la Actividad Sanitaria de los S.P.
- Reglamentos Específicos
- Reglamentos Específicos que hacen referencias a la Vigilancia de la Salud de Trabajadores Expuestos a determinados Riesgos.
- Otros Reglamentos específicos Anteriores a la Ley de P.R.L.
- Normativa Sectorial
- Normativa de Aplicación a las Mutuas de A.T. /E.P. de la Seguridad Social
- Normativa Autonómica Sobre Asistencia Medico-Farmacéutica en los Servicios de Prevención
- Normativa Sobre Confidencialidad de Datos Médicos
- <http://www.msssi.gob.es/ciudadanos/saludAmbLaboral/saludLaboral/normativa.htm#normativa> Confidencialidad Datos Médicos

B: Normativa sobre confidencialidad de datos médicos

- Constitución Española Artículo 18.
- Ley 14/86, General de Sanidad. Artículos 10.3, 23 y 61.
- Ley Orgánica 15/99, de 13 de diciembre. de protección de datos de carácter personal.
- Real Decreto 994/1999, de 26 de junio. y Resolución de 22 de junio de 2.001
- 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.
- NTP 471: La vigilancia de la salud en la normativa de prevención de riesgos laborales
- http://www.insht.es/InshtWeb/Contenidos/Documentacion/FichasTecnicas/NTP/Ficheros/401a500/ntp_471.pdf
- La Historia Clínico- laboral: Custodia y confidencialidad de los datos de salud del trabajador. Autor: Ballester Roca. Mónica
- <http://pdfs.wke.es/8/3/5/3/pd0000018353.pdf>
- Intimidad de la persona y confidencialidad de datos en el marco de la vigilancia de la salud. el respeto a los derechos del trabajador en los reconocimientos médicos

Javier Fernández Costales Catedrático de Derecho del Trabajo y Seguridad Social. (Disponible en internet:

<https://dialnet.unirioja.es/descarga/articulo/2668748.pdf>

La confidencialidad de los datos relativos a la Vigilancia de la salud (pág. 97 y siguientes)

- Código internacional de Ética para los profesionales de la salud ocupacional
http://www.bvsde.paho.org/cursoa_epi/e/lecturas/mod6/codigo.pdf

BIBLIOGRAFÍA:

- Tratado de Medicina del Trabajo de D. Fernando Gil Hernández
- El derecho a la intimidad en los reconocimientos médicos de la LPRL desde los pronunciamientos del Tribunal Constitucional. Juana María Serrano García.
- Profesor Enrique Villanueva. Curso de Ética Médica del CGOMC.
- Código de Deontología Médica del CGOMC
- MC-Prevención
- Blog de D. Ricardo de Lorenzo
- Prevemont. Sociedad de Prevención.

**PROBLEMÁTICA DE LA CONFIDENCIALIDAD EN
LOS DIFERENTES MEDIOS DE LA MEDICINA:
EN INVESTIGACION**

Dña. Paloma Moyano López

Coordinadora del CICAB

INVESTIGACIÓN CLÍNICA

La investigación clínica es uno de los pilares fundamentales de las ciencias biosanitarias. Mediante la investigación clínica se genera conocimiento de alta calidad que permite desarrollar nuevas herramientas terapéuticas y optimizar las herramientas ya disponibles, de manera que se contribuye a la prevención, el alivio y la curación de las enfermedades, mejorando por tanto de la calidad de vida de la población.

A menudo, debido a la fuerte carga asistencial existente y a la exigencia inherente del método científico, la investigación clínica es relegada a un segundo plano en el día a día de los profesionales sanitarios.

La confidencialidad es el derecho que tienen los pacientes a que el personal sanitario no revele sus datos de salud sin su consentimiento expreso; los datos de salud forman parte de la intimidad de las personas y son merecedores de especial respeto. Es por ello que al igual que en todos los ámbitos de la vida sanitaria, la investigación clínica debe desarrollarse en un entorno que como prioridad absoluta garantice la protección de todos los sujetos participantes.

REGULACIÓN INVESTIGACIÓN CLÍNICA

La normativa reguladora aplicable en materia de investigación clínica y concretamente en ensayos clínicos, es extensa y variada, entre otros destacan:

- La Declaración de Helsinki.
- Las Normas de Buena Práctica Clínica.
- Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos.
- Ley 14/2007, de 3 de julio, de Investigación biomédica.
- Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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.

Las normas aplicables a nivel internacional y que son considerados el manual básico de la ética en la investigación son las Normas de Buena Práctica Clínica, aprobadas por la Conferencia Internacional de Armonización, todo investigador que vaya a participar en un ensayo clínico a nivel mundial debe estar obligatoriamente certificado de forma oficial en el conocimiento de las Buenas Prácticas Clínicas. Las Normas de Buena Práctica Clínica incluyen epígrafes específicos referentes a la confidencialidad en el uso de los datos de investigación.

Una situación que se pone de manifiesto de manera frecuente en materia de protección de datos y particularmente, en el tratamiento de datos de salud en los ensayos clínicos, es la concurrencia de normas como la Ley Orgánica de Protección de Datos, con normativas sectoriales, produciéndose situaciones, en la que el obligado por la norma conoce la normativa sectorial pero ignora la normativa de protección de datos específica.

PRINCIPIOS ÉTICOS INVESTIGACIÓN CLÍNICA

Los principios generales de la bioética que también rigen en investigación clínica son:

- Principio de beneficencia: obrar en función del mayor beneficio posible para el paciente.
- Principio de no-maleficencia: es la formulación negativa del principio de beneficencia.
- Principio autonomía: se basa en respetar los valores decisiones de cada persona.
- Principio de justicia: dar a cada quien lo que necesita y no exigir más de lo que puede ofrecer.

Estos principios constituyen un marco básico y un lenguaje común para analizar y resolver los conflictos éticos en el campo sanitario y por extensión en investigación.

La confidencialidad, la intimidad y la privacidad se enraízan en el principio de autonomía y la libertad individual porque cada individuo por el hecho de serlo, es gestor de sus derechos y libertades. Este derecho también implica la confidencialidad de la información recogida, es decir, la protección de sus datos.

PROCESO DE CONSENTIMIENTO INFORMADO (CI)

La expresión máxima de la autonomía del paciente y la base ética de la investigación clínica es el proceso de consentimiento informado, se trata de la expresión libre y

voluntaria por parte de un sujeto de su voluntad de participar en un ensayo clínico o proyecto de investigación determinado, tras haber sido informado de todos los aspectos del mismo que sean pertinentes para su decisión de participar o, en el caso de los sujetos menores o incapaces, una autorización o acuerdo de sus representantes legalmente designados de incluirlos en el ensayo clínico.

Debe resaltarse que el consentimiento informado no se trata simplemente de la firma de un documento por parte del paciente y el responsable médico que le proporciona la información, sino que comprende todo un proceso continuo de flujo información entre ambos que continúa durante todo el tiempo que dure la investigación, comenzando antes de que el paciente otorgue su conformidad de participación y terminando cuando el sujeto finalice su participación.

La participación en un ensayo clínico supone la cesión por parte de los paciente de su información personal para los fines recogidos en la investigación, por tanto dentro de la información proporcionada por los profesionales de salud a los pacientes para que estos tomen su decisión de participar o no debe estar incluida la relativa al tratamiento de la confidencialidad de sus datos. El paciente debe ser consciente durante el proceso de consentimiento informado que esta cesión es uno de los requisitos necesarios para su participación.

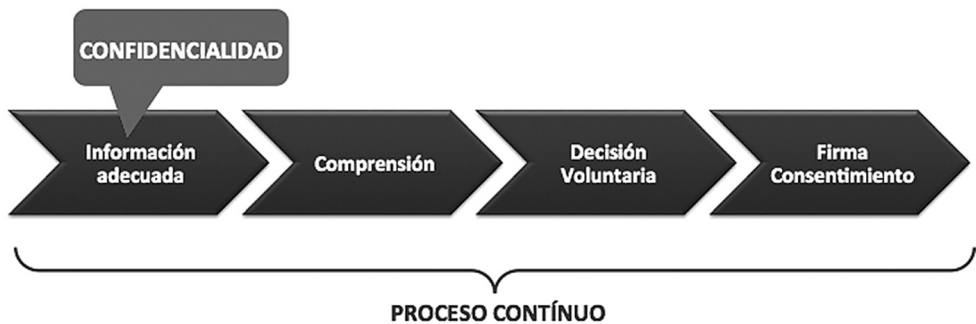


Figura: proceso de consentimiento informado

CONFIDENCIALIDAD EXPRESA EN EL CONSENTIMIENTO INFORMADO

Los sujetos incluidos en ensayos clínicos dan su consentimiento expreso de forma escrita para autorizar el uso los datos de carácter personal con los fines que establece la investigación. La información recogida sobre su salud y su tratamiento en relación con el estudio es confidencial, tal y como establece la ley. En el documento de con-

sentimiento informado debe ir reflejada la información relativa al tratamiento confidencial de los datos, debiendo quedar bien claros los siguientes puntos:

- **Identificación codificada:** al sujeto participante se le asignará un número/código del estudio. Los documentos de la investigación se identifican con el número de sujeto del estudio. En este historial no aparecerá ningún dato que permita identificarle como su nombre, iniciales, dirección, etc. Su identidad no será revelada excepto con su permiso, a no ser que sea absolutamente necesario para su seguridad.
- **Envío y publicación de información:** la información del estudio podrá publicarse o enviarse a las autoridades reguladoras o las compañías aseguradoras sanitarias de su país y de otros países en que se necesite la aprobación oficial del medicamento. La identidad no será revelada excepto con el permiso del sujeto y en caso de que sea absolutamente necesario para su seguridad.
- **Acceso a la información a terceros:** con el fin de comprobar los procedimientos y la veracidad de la información del estudio clínico, el promotor, sus representantes designados, monitores, autoridades sanitarias y comité de ética de investigación clínica independiente, tendrán derecho a revisar la información médica del sujeto sin infringir la confidencialidad. Estos accesos habilitados existen en la propia Ley LOPD.
- **Autorización al procesamiento/envío de sus datos codificados** en una base de datos. El sujeto autoriza el procesamiento de sus datos personales codificados en una base de datos, así como el envío total o parcial de estos a personas y organizaciones de fuera de su país, incluso a lugares en los que la legislación de protección de datos sea menos estricta. Sin embargo, el promotor del estudio se encargará de que, en todo momento, se mantenga al menos el mismo nivel de protección de los datos que el establecido por las leyes anteriormente mencionadas.
- **Acceso a sus datos:** a excepción de datos acerca del medicamento hasta el final del estudio o en casos de seguridad. El sujeto tiene derecho a solicitar el acceso a la información médica, corregir errores, oponerse y cancelar datos. No obstante, para garantizar la integridad científica del estudio, usted está de acuerdo en que posiblemente no tenga la posibilidad de examinar registros que identifiquen qué tratamiento del estudio en particular está recibiendo hasta que haya finalizado el estudio y sean analizados los datos, aunque su médico del estudio tendrá acceso a esta información si es necesario en caso de urgencia médica

- **Participación Sub-estudios:** se refieren a la recogida de datos adicionales a los que establecen los objetivos de la investigación, siempre será OPCIONAL la participación y así debe quedar así especificado en el documento de consentimiento. Por ello, toda información adicional a la específicamente necesaria para el desarrollo del estudio, requerirá un consentimiento a parte.
- **Derecho a la revocación** de consentimiento. En todo momento el sujeto puede revocar su consentimiento a la participación en el estudio, sin tener que dar ninguna explicación ni que esta decisión repercuta en su asistencia.

PARTES IMPLICADAS EN INVESTIGACIÓN CLÍNICA

Las partes implicadas en la realización de un ensayo clínico son:

- El *sujeto participante* en la investigación.
- El *promotor*: individuo, empresa, institución y organización responsable del inicio, gestión y/o financiación de un ensayo clínico o proyecto de investigación.
- El *equipo investigador* encargado de la realización de la investigación en un centro.
- El *monitor*: persona externa contratada por el promotor que nunca puede formar parte del equipo investigador y se encarga de verificar el correcto cumplimiento de las normas éticas y legales de la investigación clínica, asegurando en primer lugar la protección de los paciente; sirve de vínculo entre el promotor y el investigador principal cuando estos no concurren en la misma persona.

La propia legislación específica anteriormente mencionada, refleja el hecho de que en investigación clínica entran en juego participantes externos a las instituciones sanitarias donde se realiza la investigación, esto resalta aún más la importancia del el mantenimiento de la confidencialidad, debiendo cuidarse de manera escrupulosa. Tanto El acceso de estos agentes externos a la información clínica como el tratamiento que se dará a los datos recogidos, debe ir correctamente especificado en el contrato firmado entre el centro, el promotor y el investigador.

Desde el punto de vista de la protección de datos, las relaciones entre los participantes se configuraran habitualmente de una forma independiente, de forma que el investigador sea responsable de determinados aspectos del tratamiento de datos y el promotor de otros, debiendo existir cláusulas que permitan esa comunicación de la información.

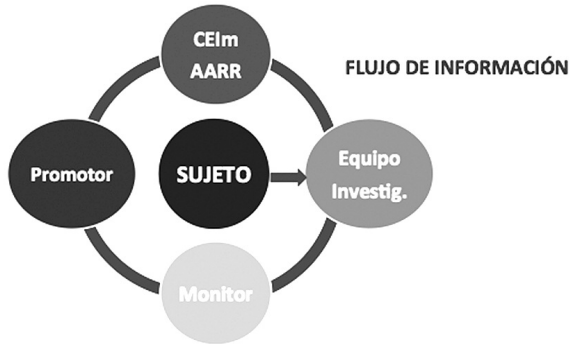


Figura: Flujo de información en un ensayo clínico.

ACCESO A LOS DATOS PERSONALES

Los distintos implicados en investigación clínica, tienen acceso de forma desigual a los datos confidenciales de los sujetos participantes, estos accesos quedan reflejados en la siguiente figura



Figura: acceso de las partes implicadas a los datos.

El acceso a la historia clínica por parte de terceros según la ley orgánica de protección de datos está muy limitado. En los casos de investigación referente a ensayos clínicos, en la actualidad la mayoría de los centros que cuentan con historia clínica electrónica aun no están preparados para proporcionar accesos de “visualización/investigación”

a aquellas personas que a pesar de ser externas al personal sanitario habitual, legalmente están autorizadas para ello, por ejemplo coordinador de ensayos clínicos, personal de enfermería o monitor. Este asunto está experimentando una evolución en los últimos años a nivel nacional, con el cambio de la historia clínica al formato electrónico, en muchos centros sanitarios se está proporcionando este tipo de accesos.

CONFIDENCIALIDAD DE LOS DATOS DISOCIADOS

- En referencia a la disociación de datos, deben resaltarse los siguientes puntos:
- El investigador es el responsable de la disociación de los datos.
- El modo de disociación es mediante la asignación a cada sujeto un código numérico o alfanumérico según un esquema de aleatorización.
- La información del cuaderno de recogida de datos y las notificaciones que se envíe al promotor irá identificadas mediante el código.
- El investigador custodia la relación de datos identificativos y códigos de disociación, accediendo a ellos el monitor, auditor e inspector.
- El promotor no accederá nunca a los datos personales, pero es responsable del tratamiento que se le da a los mismos.
- El monitor solo visualizará los datos a los que acceda, sin registrarlos en ningún caso.
- El auditor, accederá a los datos de los sujetos, sin registrarlos, con fin de comprobar el cumplimiento del protocolo y normativa aplicable.
- Los Promotores una vez aplicado el procedimiento de disociación, podrán comunicar libremente los datos disociados a otras personas físicas y jurídicas.

DISOCIACIÓN DE DATOS EXTERNALIZABLES INVESTIGACIÓN CLÍNICA

Al igual que en casi todos los ámbitos, la globalización ha jugado un papel importantísimo en la investigación clínica. En la actualidad, una gran parte de los ensayos clínicos realizados tiene carácter internacional, eso implica que haya un gran número de investigadores y centros, existiendo por tanto una gran heterogeneidad en la información que se recoge, ya que cada uno de los centros puede que utilice distintas técnicas para analizar por ejemplo los valores analíticos, añadiendo a ello la subjetividad inherente que existe a la hora de evaluar determinados datos que pueden

ser fundamentales para los objetivos de investigación como pruebas funcionales, evaluaciones radiológicas, etc. Para evitar sesgos en la investigación y procurar la mayor homogeneidad de los datos posibles, la evaluación de este tipo de pruebas suele centralizarse en centros de referencia, por ejemplo las evaluaciones analíticas de todos los centros participantes se analizan en laboratorios centrales, en lugar de en laboratorios locales, los ECG son validados por cardiólogos de referencia del ensayo clínico a nivel internacional, las evaluaciones radiológicas de imágenes deben enviarse para su supervisión a servicios centrales, etc. Otro de los factores que pueden llevar a la externalización de datos es la falta de recursos en el centro para realizar determinadas técnicas y evaluaciones requeridas en el estudio. Todo ello implica el envío de muestras/pruebas a agentes externos a los centros donde se realiza la investigación, por lo que es de vital importancia que los datos que se exporten, independientemente del formato que tengan, siempre aparezcan codificados para no vulnerar la confidencialidad.



Figura: pruebas centralizadas en ensayos clínicos

PROBLEMAS DE LA CONFIDENCIALIDAD EN INVESTIGACIÓN CLÍNICA

Algunos problemas de confidencialidad en la realización de ensayos clínicos son los que se describen a continuación:

- **Tiempo insuficiente en el proceso de consentimiento informado.** El paciente no entiende bien cuáles son los requisitos de cesión de datos. Los formularios de consentimiento informado no describen detalladamente el tratamiento de la confidencialidad o no reflejan de manera clara cuales son los datos adicionales solicitados y el paciente firma de forma mecánica la participación en sub estudios opcionales.

- **Faltas de Confidencialidad** dentro el equipo multidisciplinar, por ejemplo dar el nombre del paciente a un monitor en una conversación telefónica en lugar del código
- **Estudios internacionales:** la participación en investigación clínica a nivel mundial puede generar fugas de datos confidenciales. Por norma general el material proporcionado por los promotores suele ser la misma para todos los centros del mundo y la información requerida en ellos idéntica, sin embargo la legislación en cuestión de protección de datos no es la misma en todos los países; hay países en los que las iniciales de los sujetos son considerados datos de carácter personal y no puede enviarse ningún documento que las contenga fuera del centro, mientras que en otros países está permitido su uso. El ejemplo de las iniciales de los sujetos es un punto muy común puesto que en casi todos los documentos de ensayos internacionales aparecen como campo a rellenar en los cuadernos de recogida de datos, formularios de extracciones, etc; si el encargado de cumplimentar estos documentos sea un persona sin formación probablemente rellenará estos campos e incurrirá en una violación de la confidencialidad.
- **Errores de la codificación:** la codificación requerida en los ensayos clínicos puede llevar a errores, asignado en el envío de una muestra un código correspondiente a otro paciente, algunas de estas situaciones no tienen trascendencia y son solucionables al ir acompañados de algún dato personal que permita al personal del centro/promotor verificar que se trata del paciente correcto, como por ejemplo año de nacimiento, fechas de inicio de tratamiento, etc. Sin embargo hay algunos casos en los que el error puede tener repercusiones muy importantes que pueden poner al paciente en una situación de peligro derivadas de decisiones tomadas en base a diagnósticos erróneos por cruce de resultados.
- **Accesos** indebidos a la historia clínica debido a la restricción de accesos.
- **Externalización de los datos de pruebas:** fuga de datos por una mala codificación o anonimización. Ejemplo, envío de un ECG con el nombre del paciente.

PROCEDENCIA	PROBLEMA	SOLUCIÓN
PROCESO DE CONSENTIMIENTO INFORMADO	<ul style="list-style-type: none"> • Firma del paciente sin entender información • Tiempo dedicado insuficiente • Formulario con información inadecuada 	<ul style="list-style-type: none"> • Cualificación del equipo investigador • Dedicar el tiempo requerido
ENVÍO EXTERNO DE PRUEBAS	<ul style="list-style-type: none"> • Violación confidencialidad: envío datos personales • Errores codificación • Diagnósticos erróneos: resultados cruzados 	<ul style="list-style-type: none"> • Profesionales cualificados para el uso de herramientas necesarias • Formación del equipo investigador • Dedicar el tiempo requerido
ESTUDIOS INTERNACIONALES CUMPLIMENTACIÓN CRDs	<ul style="list-style-type: none"> • Diferente legislación internacional • Material de estudio común para todos los países 	<ul style="list-style-type: none"> • Formación del equipo investigador
HISTORIA CLÍNICA	<ul style="list-style-type: none"> • Accesos indebidos • Limitación de accesos a terceros 	<ul style="list-style-type: none"> • Implementación de acceso de investigación (visualización) a terceros y a perfiles sanitarios/investigación tradicionalmente no permitidos

Tabla: problemas y soluciones

**PROBLEMÁTICA DE LA CONFIDENCIALIDAD EN
LOS DIFERENTES MEDIOS DE LA MEDICINA:
HOSPITALES**

Dr. D. Jorge Mariño Del Real

Jefe del Servicio de Urología. HIC. (Badajoz)

La propia legislación específica anteriormente mencionada, refleja el hecho de que en investigación clínica entran en juego participantes externos a las instituciones sanitarias donde se realiza la investigación, esto resalta aún más la importancia del mantenimiento de la confidencialidad, debiendo cuidarse de manera escrupulosa. Tanto El acceso de estos agentes externos a la información clínica como el tratamiento que se dará a los datos recogidos, debe ir correctamente especificado en el contrato firmado entre el centro, el promotor y el investigador.

Los Hospitales son un componente importante del sistema de atención de salud. Son instituciones sanitarias que mediante personal sanitario y otros profesionales, y de instalaciones para el ingreso y atención a los pacientes, ofrecen servicios médicos, de enfermería y otros servicios relacionados durante las 24 h del día, los 365 días del año.

Ofrecen una gran diversidad de servicios de atención aguda, crónica, cuidados paliativos, con los medios diagnósticos y terapéuticos necesarios para responder a manifestaciones agudas y crónicas debidas a enfermedades, así como a traumatismos, anomalías genéticas, etc.

Por sus características antes comentadas, en los hospitales existe un gran flujo de información “sensible” que circula de un lado a otro, manejada por un gran número de profesionales de diversa índole, información que es necesaria salvaguardar en aras del derecho de confidencialidad de los seres humanos, y en base a la obligatoriedad del secreto médico por parte de los profesionales sanitarios.

Debido a la ingente cantidad de información que se maneja y la complejidad organizativa de los centros sanitarios, en nuestra práctica diaria podemos tener conflictos de valor relacionados con los derechos a la intimidad y confidencialidad, y a la guarda del secreto profesional. Estos conflictos pueden ser de diversa índole, y es necesario que los profesionales sanitarios tomemos conciencia de ellos, y aprendamos cuál es el modo más óptimo de manejarlo en la práctica y de resolver el conflicto de valores que entraña. No siempre lo que nos parezca mejor desde el punto de vista ético, será aceptable o no jurídicamente, pero en cualquier caso, siempre será necesario saber con exactitud qué dice la ley y tener muy en cuenta sus prohibiciones.

Veamos a continuación algunos de los principales conflictos que surgen en nuestros hospitales, y que son transversales a otros medios de la medicina:

SECRETO PROFESIONAL Y DEBER DE PROTECCIÓN DE LA VIDA DE TERCEROS.

Podemos tener conflictos de este tipo por ejemplo en la atención de pacientes psiquiátricos agresivos o con ideas de autolisis, o con enfermedades infectocontagiosas.

En estos casos se contraponen la protección de la vida de las personas y el derecho que el paciente tiene al respeto de su intimidad y confidencialidad de sus datos. Lo ideal en estos casos es, intentando salvaguardar la relación de confianza entre el médico y el paciente, en el primer caso realizar el tratamiento voluntario y ambulatorio del paciente con el fin de controlar sus síntomas, o el tratamiento ambulatorio forzoso, en el caso de negativa del paciente, o incluso si es necesario en internamiento voluntario o forzoso.

En el segundo caso, si tras el apoyo emocional al paciente no se convence de la necesidad de tomar medidas de protección para evitar el contagio de su pareja, el médico propondrá las medidas de protección a la pareja mediante entrevista personal, intentando no romper el secreto profesional. Si consideramos que aun así no es suficiente y la persona tiene riesgo de contagio, se le comunicaría el riesgo directamente a la persona, incluso si fuera necesario el médico podría denunciar a las autoridades sanitarias ante un presunto delito de lesiones.

ACTUACIÓN DE LOS PROFESIONALES EN PROCESOS JUDICIALES COMO PERITOS O TESTIGOS.

Ante un requerimiento judicial para actuar como peritos o testigos, debemos acudir al requerimiento judicial en el caso de ser llamados como testigos, indicando al juez de la obligatoriedad de guardar secreto profesional, contestando a las preguntas intentando lesionar lo menos posible la obligación del secreto. Si somos llamados como peritos por alguna de las partes, y hemos tenido relación profesional con el paciente, dado que existe voluntariedad, podemos rechazar la petición en base al deber de secreto profesional y a la relación del médico con el paciente.

USO DE LA INFORMACIÓN CLÍNICA POR PROFESIONALES SANITARIOS O NO SANITARIOS.

La cooperación "horizontal" tanto intraprofesional (entre médicos) como interprofesional (entre distintos profesionales que colaboran en unidades de atención clínica) exige compartir gran cantidad de información clínica que se utiliza para la atención del paciente. También la cooperación "vertical" entre distintos niveles exige compartir información. Así mismo, a veces es necesario compartir información entre distintos sectores (educativos, judicial, social, etc). Es necesario que en las instituciones sanitarias desarrollemos una cultura de compartir en mínimo de información que ofrezca el máximo beneficio, y que pueda provocar el menor daño posible.

No obstante, hoy en día, con el uso de la historia clínica electrónica, y el acceso a la información de manera selectiva según el nivel asistencial, en gran medida se ha solucionado esta problemática.

RECHAZO DEL PACIENTE A COMPARTIR INFORMACIÓN CON FAMILIARES.

Hay que procurar siempre lesionar lo menos posible la relación médico-paciente, intentando proteger la salud y la vida de las personas sin romper el secreto médico, aunque es evidente que el deber de proteger la salud de las personas es superior que el de la guarda del secreto profesional. La educación preventiva y la comunicación recíproca, es con frecuencia la mejor arma para resolver conflictos en la práctica médica. Hay que hacer lo posible para que los pacientes sean capaces de gestionar autónomamente su vida y su salud, para que puedan protegerse sin necesidad de que esto obligue al profesional a romper el secreto.

PRIVACIDAD Y SALUD PÚBLICA.

Como ya se ha comentado anteriormente, la salud pública está por encima del deber de secreto profesional y confidencialidad. Debemos intentar proteger la salud pública salvaguardando la intimidad y, al mismo tiempo, procurar que la intimidad tampoco impida el desarrollo de la salud pública. En cuanto a la investigación humana, debemos respetar siempre los principios éticos que la rigen.

COMENTARIOS PERSONALES EN LA HISTORIA CLÍNICA Y ACCESO A LA MISMA.

Cuando el paciente solicita que se le entregue la historia clínica, el médico debe informarle que no es posible darle información relativa a la confidencialidad de terceras personas cuyos datos consten en la historia clínica, ni las anotaciones subjetivas que el personal médico haya hecho constar. Se le entregará al paciente una copia de la historia sin aquellos datos protegidos. Se le podrá entregar la información relacionada con terceras personas, en el caso de que éstas den su consentimiento para hacerlo.

ACCESO A DOCUMENTACIÓN CLÍNICA POR ADMINISTRATIVOS Y PERSONAL LABORAL.

La mayoría de los centros sanitarios cumplen las normas legislativas en materia de confidencialidad de datos, y en caso de detectarse dificultades para el cumplimiento,

debe ponerse en conocimiento de la dirección del dentro. Es necesario tratar bien la información para salvaguardar la confidencialidad de los datos. La información en papel debe vehiculizarse en sobres cerrados, usando lo menos posible el fax. Con la llegada de la historia clínica electrónica y el menor uso del papel en nuestros centros, se ha solucionado en gran medida esta problemática.

CERTIFICADOS DE DEFUNCIÓN.

En España es legalmente preceptivo hacer constar el diagnóstico en los certificados de defunción, a diferencia de otros países de Europa. Debería instarse a las organizaciones representativas para que promueva cambios legislativos que eviten poner las causas de defunción en el certificado, quedando los datos precisos registrados en donde pueda garantizarse su confidencialidad.

Debido a su tamaño y características específicas, hay algunos conflictos de valor que pueden darse con mayor frecuencia en el medio hospitalario, como pueden ser:

HISTORIA CLÍNICA: ACCESIBILIDAD Y PROTECCIÓN.

Tradicionalmente hemos tenido archivadas las historias clínicas de los pacientes ingresados en distintas partes de las plantas de hospitalización, de los consultorios, etc, y prácticamente cualquier trabajador del hospital tenía acceso a ellas. Incluso en muchas ocasiones, hemos dejado documentación clínica en los controles de enfermería o en determinados sitios, que hacían accesible estos datos incluso a los propios enfermos o familiares. Nos parece lógico y normal que cualquier profesional consulte información de algún compañero, conocido o amigo que se encuentre ingresado, ya sea documentación clínica o estudios de imagen, a pesar de no tener ninguna relación de atención médica con el mismo, sabiendo que nuestro código deontológico en su artículo 27 expresa claramente, que el hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional.

Es evidente que la historia clínica en la principal causa de vulneración del secreto profesional y del derecho a la confidencialidad del paciente. Es necesario arbitrar medidas para que esto no suceda, haciendo un correcto uso de la información clínica.

Con la llegada de la historia clínica electrónica, con sus garantías y sistemas de seguridad que luego comentaremos, existe menos posibilidad del mal uso y acceso a esta información.

HISTORIA CLÍNICA ELECTRÓNICA.

Es evidente que la historia clínica electrónica es un sistema seguro y eficaz, que ha solucionado gran parte de la problemática existente en cuanto a la accesibilidad y protección de los datos clínicos. Son bases de datos encriptados, con altos niveles de seguridad, a las que se accede mediante identificación inequívoca del profesional y del paciente. La existencia de distintos niveles de acceso, hace que cada profesional entre en contacto con la información que debe manejar en función de su puesto de trabajo.

INFORMACIÓN A FAMILIARES Y ALLEGADOS.

De todos es conocido que el enfermo es la persona a quien debe informar en primer lugar el médico de lo referente a su estado de salud. Sus familiares y allegados sólo tienen derecho en determinados casos a saber lo que concierne a la salud del enfermo, aunque generalmente se presume que el enfermo no quiere ocultarles nada de su estado.

No puede darse información clínica a una tercera persona. Es normal que los hijos se interesen por lo que le sucede a los padres, y viceversa, y soliciten información sin la presencia del interesado. En estos casos se debería tener la autorización expresa del paciente.

Muchas veces tenemos paciente ingresado en habitaciones múltiples, unidades de reanimación, etc en las que no es fácil mantener la confidencialidad con el paciente. Debemos en estos casos tratar de informar de una manera más “general”, intentando reservar la información más “sensible” para un momento y situación en la que sea más fácil salvaguardar la confidencialidad.

EXCESO DE LOCUCIDAD DEL PERSONAL SANITARIO.

Respeto a los comentarios sobre la salud de los pacientes realizados en pasillos, ascensores, cafetería, etc. Hay que tener en cuenta que el hecho de que el interlocutor sea médico o enfermero no libera de la obligación de sigilo. No se deben hacer comentarios con amigos o conocidos sobre el estado de salud de terceras personas identificables. El deber del secreto no sólo alcanza a aspectos médicos del paciente, sino a otros aspectos de la vida del paciente que se hayan podido conocer o de terceras personas con quien se relaciona.

Podemos concluir, que en los hospitales, debido a sus dimensiones y características específicas, existes en muchas ocasiones problemas en cuanto a la confidencialidad y el secreto profesional.

En relación a ello, debemos conocer y aplicar lo que dice el artículo 27 del CDM: el hecho de ser médico, no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional; en las instituciones sanitarias los directivos velarán por una clara separación entre documentación clínica y administrativa; el médico preservará en su ámbito social, laboral y familiar, la confidencialidad de los pacientes.

En muchas ocasiones, se trata de aplicar en nuestra práctica diaria, el menos común de los sentidos, que es el “sentido común”, y que hagamos un buen uso de la historia clínica y tratemos bien la información.

BIBLIOGRAFÍA.

1. Código de Deontología Médica. Guía de Ética Médica. Capítulo V: Secreto médico. Madrid: Consejo General de Colegios Oficiales de Médicos, julio 2011.
2. Bátiz Cantera J., Casado Blanco M., Casado Gómez T., Castellano Arroyo M., Ciprés Casasnovas L., Collazo Chao E., et al. Secreto Profesional del Médico. En: Manual de Ética y Deontología Médica. Madrid: Organización Médica Colegial de España. 2012; p. 97-112.
3. Servicio Extremeño de Salud. Reglamento de uso de la historia clínica. Badajoz: Consejería de Sanidad y Consumo. Diciembre 2005.
4. Menéndez de Lucas, J.A. Cuestiones médico-forenses en la práctica clínica. Madrid: Máster Line, S.L. Marzo 1999.
5. Bertrán J.M., Collazo E., Gérvás J., González Salinas P., Gracia D., Júdez J., et al. Intimidad, confidencialidad y secreto. Guía de ética en la práctica médica. Madrid: Fundación de Ciencias de la Salud. 2005.
6. Castell Arteche, J.M. El derecho a la confidencialidad. Protección de datos. Derecho a la intimidad. El secreto médico. Cuarto congreso de derecho y salud. Los derechos de los usuarios de los servicios sanitarios. San Sebastian. Noviembre. 1995.
7. Álvarez-Cienfuegos Suarez, J.M., López Domínguez, O. Secreto Médico y Confidencialidad de Datos Sanitarios. En De Lorenzo y Montero, R (Coordinador General) Plan de formación en responsabilidad legal profesional. Unidad didáctica número 4. Madrid: Edicomplet. Asociación Española de Derecho Sanitario. 1998.
8. Romeo Casabona, Carlos M., Castellano Arroyo, Maria. La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica. DS. Vol 1, Núm. 1, Julio-Diciembre. 1993.
9. Castellano Arroyo M. Problemática de la Historia Clínica. Seminario conjunto sobre Información y Documentación Clínica. . Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo. Madrid. Septiembre 1997.
10. Júdez J., Nicolás P., Delgado M.T., Hernando P., Zarco J., Granolleres S. Confidencialidad en la práctica clínica, la historia clínica y la gestión de la información. En: Gracia d., Júdez J. Ética en la práctica clínica. Madrid: Triacastela. 2004; p. 75-126.

**PROBLEMÁTICA DE LA CONFIDENCIALIDAD EN
LOS DIFERENTES MEDIOS DE LA MEDICINA:
FORMACION**

Dr. D. Carlos López Bernáldez

Profesor Asociado en Ciencias de la Salud.

Facultad de Medicina UEx. (Badajoz)

Secreto Médico Compartido

Básicamente es el Secreto que resulta de compartir un hecho conocido con otro profesional o colega. Teniendo presente como objetivo primordial el que esto redunde en beneficio terapéutico del paciente.

Deber de reserva que obliga a todas las personas que, en el ejercicio de su labor profesional, por participar directa (compartido) o indirectamente (derivado) en la atención sanitaria de un paciente, llegan a conocer información relativa a ésta.

El secreto médico compartido obliga a toda persona (otros médicos del equipo, enfermeras, matronas, trabajadores sociales,...) que, por su actividad profesional, está implicada directamente en la atención sanitaria del paciente junto al médico responsable del proceso asistencial. A diferencia del Secreto médico derivado: consecuencia de la complejidad que tienen actualmente los centros asistenciales, obliga a toda persona que, sin participar directamente en la atención sanitaria del paciente, por su labor, necesaria para el correcto funcionamiento del centro (administrativos, técnicos, auxiliares de limpieza,...) pueden llegar a conocer datos confidenciales de una persona o personas allí atendidas. Es deber del responsable o responsables institucionales que todos los colaboradores asistenciales conozcan y cumplan con su obligación de reserva.(1)

Ahora bien, no supone ninguna violación del deber de secreto, la transmisión de información relativa al paciente a otros facultativos o profesionales sanitarios en el medio clínico, cuando es necesaria para la realización de pruebas o de otros tratamientos acompañantes, tal y como establece la Ley General de Sanidad en su artículo 61, o al personal administrativo en todo lo necesario para el desempeño de su función, sin olvidar que todos ellos están obligados del mismo modo por un deber de secreto compartido.(2)

Existen situaciones que pueden considerarse un alejamiento de la confidencialidad:

- judiciales.
- epidemiológicos,
- de salud pública,
- de investigación,
- de docencia,
- de información y estadística sanitaria.

Estas situaciones constituyen diferentes formas del secreto profesional compartido o derivado

Confidencialidad en la actividad asistencial docente

La importancia que en el estado de derecho tiene garantizar el amparo a la intimidad que el paciente se ve forzado a delegar dentro del entorno del sistema sanitario está cubierta con 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 establece en su artículo 7, cuando hace referencia al derecho a la intimidad:

- 1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.*
- 2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos sanitarios de los pacientes.”*

Por todo ello, se hace necesaria una regulación que ampare con garantías de calidad el acceso a la información sanitaria tanto para la formación de Grado y en la formación sanitaria especializada (MIR) como en las labores investigadoras. La socialización de la medicina y un trabajo en equipo cada vez más usual condiciona que sean varios profesionales, alumnos y médicos en formación a la vez los que conozcan todas peculiaridades de la vida y enfermedad del paciente.

Igual importancia tiene la realización dentro de las Facultades de Medicina, Comisiones de Docencia, en Centros de Salud y Hospitales de actividades educativas y de estímulos, que marquen en los discentes unos hábitos de conducta que mantengan intacto el derecho a la intimidad de los pacientes. Corresponde a las Autoridades Sanitarias, Facultades de Medicina, Comisiones de docencia, Jefes de Departamento, Profesores Vinculados o Asociados o Colaboradores, Tutores clínicos a través tanto de sus programas docentes como en la actividad asistencial/formativa diaria la responsabilidad de informar y velar por la creación de estos hábitos en alumnos y médicos en formación, así como el cumplimiento de la normativa que rige el funcionamiento del Centro y de las medidas de protección de datos.

Los alumnos y médicos en formación deberán cumplir las normas de uniformidad e identificación de forma visible que informen a los pacientes y a los demás profesionales del centro que van a intervenir en su proceso asistencial.

Varias disposiciones sanitarias regulan la actividad asistencial de los médicos en formación, MIR.:

El Real Decreto 183/2008, de 8 de febrero, por el que se determinan y clasifican las especialidades en Ciencias de la Salud y se desarrollan determinados aspectos del sistema de formación sanitaria especializada establece que *“El sistema formativo de residencia implicará la asunción progresiva de responsabilidades en la especialidad que se esté cursando y un nivel decreciente de supervisión, a medida que se avanza en la adquisición de las competencias prevista en el programa formativo, hasta alcanzar el grado de responsabilidad inherente al ejercicio autónomo de la profesión sanitaria de especialista”*.

El Real Decreto 1146/2006, de 6 de octubre, por el que se regula la relación laboral especial de residencia para la formación de especialistas en Ciencias de la Salud, al regular los deberes de los residentes establece que están obligados a *“Prestar personalmente los servicios y realizar las tareas asistenciales que establezca el correspondiente programa de formación y la organización funcional del centro, para adquirir la competencia profesional relativa a la especialidad y también contribuir a los fines propios de la institución sanitaria”*.

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 establece en su Artículo 16.1. Usos de la historia clínica:

“La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.”, sin necesidad del consentimiento del paciente”.

Por tanto, los residentes en formación de cualquier año, por ser personal asistencial y trabajadores del Centro, tienen derecho a acceder a la historia clínica de los pacientes implicados en las actuaciones asistenciales que realicen en cada momento. No consultar ni cumplimentar los actos asistenciales en la historia clínica puede tener repercusiones en la seguridad de los pacientes y legales por mala praxis clínico-asistencial.⁽³⁾

La referida Ley de Autonomía del Paciente en su artículo 16.3 establece que *“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 13 de diciembre, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El*

acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

La disociación de datos habrá de realizarla un profesional sanitario sujeto al secreto profesional u otra persona sujeta a una obligación equivalente de secreto.

Los alumnos de medicina solo pueden acceder a la historia clínica con los datos personales disociados, respetando la confidencialidad de los datos de salud.

El acceso a la Historia Clínica Digital del Sistema Nacional de Salud se rige por los mismos principios que se han referido para la historia clínica tradicional.

El Código Deontología Médica especifica en su artículo 28,1: *“El director médico de un centro o servicio sanitario velará por el establecimiento de los controles necesarios para que no se vulnere la intimidad y la confidencialidad”*.

Bibliografía:

- 1.- El Médico/formación_acre2004/tema11/etica1.php on line 67
- 2.- Romeo Casabona CM, Castellano Arroyo M. La intimidad del paciente desde la perspectiva del secreto médico y del acceso a la historia clínica
- 3.- Protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en ciencias de la salud, Comisión de Recursos Humanos del Sistema Nacional de Salud, ha aprobado el 26 de mayo de 2016, y publicado en el DOE.
- 4.- Casado Blanco M. Manual de Documentos Médico-Legales. Junta de Extremadura. 2008.

CON LA COLABORACIÓN DE

