Decálogo de buenas prácticas para la protección de datos en Medicina del Trabajo y vigilancia de la salud

Gloria Llanes - Fernández de la Cueva[1], David Bejarano - Álvarez[2], Lourdes María Márquez - Rodríguez[3]

[1]Premap Seguridad y Salud. Enfermera especialista en Enfermería del Trabajo. Huelva
[2]Servicio Andaluz de Salud. Enfermero. Hospital Juan Ramón Jiménez. Huelva
Atlantic Copper. Enfermero especialista en Enfermería del Trabajo. Huelva
[3]Premap Seguridad y Salud. Enfermera especialista en Enfermería del Trabajo. Huelva

Correspondencia:
Gloria Llanes Fernández de la Cueva
C/ Antonio Borrero Chamaco. 1 3ºC
21001 Huelva.
correo electrónico: gloriallanes@hotmail.com

La cita de este artículo es: G. Llanes Fernández de la Cueva et al. Decálogo de buenas prácticas para la protección de datos en Medicina del Trabajo y Vigilancia de la Salud. Rev Asoc Esp Espec Med Trab 2016; 25: 34-42

RESUMEN

La protección de datos está presente en todo el ámbito sanitario. Médicos y enfermeros reciben formación específica en este sentido, dada la importancia que alberga unas buenas prácticas en materia de protección de datos. No obstante, no está demás recordar con cierta periodicidad una serie de cuestiones que ayudan a preservar la intimad y el secreto profesional en el ejercicio del trabajo a desempeñar.

En el ejercicio de la Medicina del Trabajo en el aspecto de la vigilancia de la salud igualmente se hace necesario salvaguardar la gran cantidad de datos sobre trabajadores y las empresas atendidas en dicha actividad preventiva. Para ello se pretende dar a conocer un decálogo de buenas prácticas sobre protección de datos en vigilancia de la salud.

Existe abundante bibliografía referente a la protección de datos en el ámbito sanitario, pero no tanta relativa a la actividad de la vigilancia de la salud dentro de la Medicina del Trabajo y la Salud Laboral.

Palabras claves: protección de datos, secreto profesional, intimidad, Medicina del Trabajo, Salud Laboral, Enfermería del Trabajo.

TEN TIPS FOR BEST PRACTICE FOR DATA PROTECCION IN OCCUPATIONAL MEDICINE AND OCCUPATIONAL HEALTH

Abstract: Data protection is a key issue for all the sanitary system. Doctors and nurses are thoroughly educated in this area due to the importance of the good practice in data protection. However, it is advisable for the medical and sanitary staff to regularly remind the basic aspects that will help to protect the confidentiality and professional secrecy.

In Occupational Health, it is also required to protect the amount of data that are managed about many workers and businesses. This is intended to provide several good practices in this way.

There are numerous references in the bibliography regarding general data protection in the healthcare system, but not so many about specific areas such as Occupational Medicine and Occupational Health.

Key words: Data protection, professional secrecy, privacy, Occupational Medicine, Occupational Health, Occupational Health Nursing.

Fecha de recepción: 18 de enero de 2016
Fecha de aceptación: 10 de marzo de 2016

Introducción

La protección de datos en ciencias de la salud se hace imprescindible, al igual que en otras disciplinas. En la vigilancia de la salud, el conocer lo que conlleva implícita la protección de datos, el secreto profesional y la vulneración de ese secreto, también se hace ineludible. Dada la escasa bibliografía existente en este sentido, se hace necesaria la creación de este decálogo centrado en el ejercicio profesional de los trabajadores dedicados a la Medicina del Trabajo y la Salud Laboral.

De manera clara y concisa, se desarrollarán las buenas prácticas en este sentido, se definirán los conceptos claves a tener en cuenta y se especificarán las penas que conllevan las malas acciones en materia de protección de datos.

Como en toda disciplina, se hace necesario definir ciertos conceptos que afectan a la materia de estudio, para que así queden aclaradas las nociones (Figura 1[1].

- Datos de carácter personal: "Cualquier información concerniente a personas físicas identificadas o identificables". Ejemplo: DNI, teléfono, nombre, apellidos, sonidos o imágenes que identifiquen al trabajador…

- Derecho a la intimidad[2]: "Potestad que tenemos de que un tercero no conozca nuestra vida privada, y también la posibilidad de controlar lo que otros conocen de nosotros mismos."

- Confidencialidad: "Lo que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas"

- Documentación clínica: "Soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial."

- Fichero: "Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso." Los ficheros pueden ser: automatizados, bases de datos informatizadas, o no automatizados, cuando los encontramos en soporte papel.

- Historia clínica: "Conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole, sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial."

Tratamiento de datos: "Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

- Responsable del tratamiento del fichero: "Es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento." Los responsables de los ficheros de datos personales, tienen la obligación de notificar su creación, modificación y cancelación a la AEPD (Agencia Española de Protección de Datos).

- Afectado o interesado: "Persona física titular de los datos que sean objeto del tratamiento a que se refiere el tratamiento de datos."

- Cesión o comunicación de datos: "Toda revelación de datos realizada a una persona distinta del interesado."

- Consentimiento: "Toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen."

- Derecho de acceso[3]: "Es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos."

- Derecho de rectificación: "Es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos."

- Derecho de cancelación: "El ejercicio de este derecho dará lugar a que se supriman los datos que resulten inadecuados o excesivos, sin perjuicio del deber de bloqueo".

- Derecho de oposición: "Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en ciertos supuestos (como consecuencia de la ocurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario)"

En España la Agencia Española de Protección de Datos[4] ha publicado la Guía de Protección de Datos en las Relaciones Laborales, entre otras con el objetivo de promover la aplicación de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter

Figura 1. Resumen de las definiciones relacionadas con la Protección de Datos.

Personal (LOPD) y del Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD. Por tanto, se ofrecen en esta guía herramientas de ayuda a organizaciones tanto públicas como privadas para un adecuado cumplimento de la legislación vigente.

Además en esta guía se analizan aspectos de la protección de datos que han planteado alguna dificultad de interpretación o aplicación práctica, tratándose en todo momento de acercar la protección de datos a la cultura empresarial y a la organización, diseño y funcionamiento de las organizaciones. Igualmente, esta guía hace referencia a la consideración de los datos especialmente protegidos que se desarrollaran a lo largo de este documento.

Como punto importante en esta guía, está el concerniente al acceso de los datos por parte de la empresa. Las facultades de acceso a la información por parte de la empresa son muy limitadas refiriéndose simplemente a conocer la aptitud o no aptitud del trabajador. No obstante, es posible que el empresario deba acceder de modo específico a algún tipo de información personal del trabajador, información que sea necesaria para el cumplimiento de sus obligaciones por tener que tomar medidas correctoras al respecto. En estos casos, la legitimación para el tratamiento deriva de la propia Ley pero se limitará a los datos estrictamente necesarios.

De todo lo expuesto anteriormente radica la importancia de que el personal dedicado a la salud laboral esté familiarizado con la protección de datos, las leyes que la regulan, el secreto profesional, la vulneración del mismo… Para todo ello, aparte de elaborar este documento informativo, se crea un decálogo de buenas prácticas en este sentido.

Sobre la protección de datos

El derecho a preservar la intimidad de la persona está recogido desde 1978 en nuestra Constitución Espa-

ñola[5]. En el artículo 18.1 se "garantiza el derecho al honor, la intimidad personal y familiar y a la propia imagen". Mantener la intimidad es permitir a la persona disponer de lo que es suyo, la libertad de mantener preservado aquello que no quiere que se sepa, sin su expreso consentimiento, a pesar del carácter anodino de la información desvelada.

Dicha intimidad constituye un pilar básico de la relación entre el equipo formado por médico y enfermero del trabajo (denominado Unidad Básica de Salud) y el trabajador. Es necesario ser conscientes de la importancia de la custodia de estos datos y de la responsabilidad que se asume al tratar con ellos, puesto que al adoptar actitudes poco prudentes, se puede llegar a vulnerar el derecho a la intimidad de las personas.

La protección de datos de carácter personal, se regula en la Ley 1/1982 de 5 de mayo de Protección Civil al Honor, la Intimidad y la Propia Imagen y en la Ley Orgánica 15/1999[6] de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD).

Ambas tienen por objeto garantizar y proteger, en lo concerniente al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente el honor y la intimidad personal y familiar que propugna la Constitución Española.

Concretamente, en la materia que nos ocupa, la LOPD especifica que:

- Las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud.
- Los resultados de la vigilancia a que se refiere el apartado anterior serán comunicados a los trabajadores afectados.
- Los datos relativos a la vigilancia de la salud de los trabajadores no podrán ser usados con fines discriminatorios ni en perjuicio del trabajador.
- El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.

No obstante lo anterior, el empresario y las personas u órganos con responsabilidades en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva.

Existen una serie de datos especialmente protegidos[1,4], como son los referentes al origen racial, a la salud y a la vida sexual; para que los datos de esta índole puedan ser utilizados, el afectado debe consentirlo expresamente, o bien, serán utilizados cuando sea absolutamente necesario para la prevención, diagnóstico, tratamiento médico y/o asistencia sanitaria, y siempre que se realice por un profesional sujeto a secreto profesional.

El médico y enfermero del trabajo tienen a su alcance multitud de datos pertenecientes a la intimidad de los trabajadores. Las Unidades Básicas de Salud son las encargadas de elaborar la historia clínica, y de salvaguardarla para evitar filtraciones a otros usuarios e incluso a otros profesionales. Además deben prestar especial atención a la filtración de datos a la empresa a la que pertenece el trabajador. Es por todo ello que para la vigilancia de la salud la protección de datos se hace imprescindible. Todo el personal debe conocer la LOPD y aplicarla, ya sea de forma aislada o formando parte de un equipo multidisciplinar.

Sobre el secreto profesional

El deber de todo profesional es guardar secreto sobre todo lo conocido en el ejercicio de sus funciones, constituyendo además un derecho, en este caso del trabajador.

La obligación de secreto en materia sanitaria se encuentra establecida en el artículo 10.3 de la Ley General de Sanidad[7], en la que se especifica que : "los usuarios tienen derecho a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público"

Figura 2. ecálogo de Protección de Datos en Vigilancia de la Salud.

El secreto profesional en la vigilancia de la salud, surge por la necesidad de que se preserven los datos sanitarios del trabajador que acude a su reconocimiento médico laboral.

Incluye todo aquello que, perteneciendo a la intimidad del trabajador, es conocido por el profesional (médico y/o enfermero) en el ejercicio de sus funciones.

Hay que guardar secreto respecto de los datos de carácter personal a los que se acceda sin divulgarlos, publicarlos, revelarlos, ni ponerlos a disposición de terceros, salvo previa indicación expresa del responsable del fichero o tratamiento, imperativo legal o mandato judicial. Esta obligación de secreto debe mantenerse por el profesional aun después de terminar sus relaciones con la entidad para la que presta sus servicios, garantizándose así que, una vez terminada la relación, guardará el mismo secreto respecto de dichos datos a los que haya tenido acceso.

Vulneración del deber de secreto[8]

El derecho a la intimidad individual y el deber de secreto de toda persona que pueda tener conocimiento de los datos del proceso asistencial, tiene diferentes repercusiones en los diversos ámbitos de Derecho:

Penal

Desvelar un secreto profesional se considera en el Código Penal, delito y está tipificado en el artículo 199.2 (siendo necesaria la denuncia de la persona afectada o de su representante legal): "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".

Adminisitrativo

La comunicación o cesión de los datos de carácter personal y la vulneración del deber de guardar secreto, está regulado en la LOPD, considerándose infracción muy grave y se sancionándose con multas de 300.000 a 600.000 euros.

Civil
Resarcimiento por los daños y perjuicios que la vulneración del deber de guardar secreto haya producido.
Laboral
Puede ser causa de despido disciplinario del trabajador, regulado en el Estatuto de los Trabajadores, artículo 54.2.

Buenas prácticas del profesional para preservar la protección de datos

Por todo lo expuesto anteriormente se crea la necesidad de orientar a los profesionales integrantes de las Unidades Básicas de Salud sobre las buenas prácticas en la protección de datos del trabajador. Es difícil en muchas ocasiones ser conscientes de lo que una acción incorrecta por nuestra parte en materia de protección de datos puede llegar a ocasionar a un trabajador. Es por ello que se presentan en forma de decálogo las buenas prácticas en la protección e datos relacionada con la vigilancia de la salud (Figura 2)[3].

1. Accesos a programas informáticos
Las empresas cuentan con un procedimiento para solicitar acceso a los sistemas de información. Ya hoy día, cualquier profesional tiene acceso a algún sistema informático plagado de informaciones confidenciales y datos tanto personales como sanitarios de los trabajadores que allí se reconocen. Para ese acceso, se facilitan usuario y contraseña que deben ser siempre personales e intransferibles, ya que las credenciales de un usuario relacionan a éste con sus acciones en los sistemas de información, y por tanto con sus responsabilidades.
De igual modo, no se pueden utilizar credenciales de acceso genéricas, ni reutilizar credenciales obsoletas. Por supuesto tampoco se puede acceder a los sistemas de información vulnerando la identificación y autenticación.
Es de especial relevancia también la elección de la contraseña. Siempre se han de seguir las premisas para que la contraseña sea segura:

- La contraseña debe contener números, letras y símbolos, a ser posible compuesta por mayúsculas y minúsculas. Así dificultaremos la tarea de averiguarla ya que tiene más de 30.000 combinaciones posibles
- No se debe utilizar en la contraseña información personal ni palabras comunes ya que son fáciles de averiguar
- La contraseña debe ser distinta para cada aplicación, aunque en algunas empresas hacen posible aunar las contraseñas para entrar en todo el sistema , esa contraseña no debe ser la misma que la que se utiliza, por ejemplo, para acceder a la cuenta bancaria.
- Es necesario que siempre se configuren las opciones de recuperación de la contraseña y se mantengan actualizadas. Es necesario tener actualizada la dirección de correo electrónico, para poder recibir en caso de restablecimiento de la contraseña, las instrucciones necesarias. Además hay programas que te permiten el restablecimiento de la contraseña con preguntas de seguridad (la respuesta debe ir encaminada a algo difícil de averiguar conociendo a la persona, o explorando sus perfiles de las redes sociales)
- Las contraseñas deben mantenerse siempre a salvo, nunca escitas ni a la vista de los demás .

Todo esto queda regulado por el RD 1720/2007 de 21 de diciembre, art. 91,93.

2. Publicación de imágenes
Es un tema cada vez más en auge debido sobre todo a la facilidad existente de recopilar imágenes con un simple teléfono móvil y dada también la rapidez con la que esas imágenes se pueden divulgar por las redes sociales llegando a miles de personas en pocos minutos. Como profesionales se debe tener en cuenta la privacidad de los trabajadores, ya que los datos de carácter personal son propiedad de su titular, no de quien los custodia. En ningún caso podemos sentirnos con el derecho de publicar imágenes de un trabajador por el simple hecho de haberlo atendido.
Esto es extensible desde las redes sociales, a una publicación en revista científica. Siempre debemos tener el consentimiento de la persona afectada por escrito para proceder a la divulgación y además, lo ideal es su rostro aparezca distorsionado y nunca se han de revelar sus datos personales.

El consentimiento informado en materia de protección de datos se regula en la LOPD 15/1999 art. 6,7.3 y 11.1.

3. Datos clínicos

Podemos encontrarnos con situaciones en las que se nos requieran datos clínicos para algún tipo de estudio, publicación, investigación… En estos casos debemos asegurarnos de que la entidad o persona que podrá acceder a los datos ha sido autorizado previamente para dicha cesión. En otros casos el profesional podría ceder los datos sin tener que identificar a los pacientes cuando las características del estudio así lo requieran. Para ceder datos fuera de la organización que nos compete, es necesaria la autorización del paciente y del responsable de fichero.

La normativa aplicable la encontramos en la Ley de LOPD 15/1999 Art. 3c, 3e, 6, 7.3, 8,10,11,21,27,33,34 y 44.

4. Destrucción de documentos

Todo documento que contenga datos personales de trabajadores así como datos clínicos concernientes a su estado de salud en algún momento de su vida o fallecimiento, deben ser destruidos de manera escrupulosa de forma que en ningún momento pueda descifrarse el contendido del documento. Para ello existen trituradoras de papel que hacen tiras de los documentos haciéndolos ilegibles . Una vez triturados los documentos se envían a las papeleras de reciclaje, colaborando así con el medio ambiente.

Lo ideal es que las administraciones tomen conciencia de la importancia de este medio material para la destrucción de los documentos, poniéndolo al alcance de todos los profesionales de forma que su uso sea fácil, cómodo y rápido.

Es importante reseñar también que cualquier documento que contenga datos personales o clínicos, debe estar guardado bajo llave o algún otro sistema parecido que imposibilite el acceso a cualquier persona sin autorización. Es habitual encontrar historias encima de las mesas, al alcance de cualquiera. Igualmente se encuentran hojas de registros de enfermería, papeles con anotaciones sobre los trabajadores…

Se debe tener presente siempre al finalizar la jornada laboral, no dejar a la vista documentos con datos personales o sanitarios. Siempre han de archivarse de manera correcta (bajo llave).

Normativa aplicable: Ley 41/2002 de 14 de noviembre, Ley 14/1986 de 25 de abril (General de Sanidad), Ley Orgánica 15/1999 de 13 de diciembre de LOPD, RD 1720/2007 de 21 de diciembre.

5. Envío de información por correo electrónico

Hay que poner atención al envío de cualquier información de carácter confidencial por correo electrónico y sobre todo cuando lo hacemos fuera de la red corporativa. El destinatario de ese correo debe ser el interesado o una persona autorizada por él y en todo caso, la información debería ir cifrada.

Incluimos también en este apartado el llevar información en CD, pen drives, o cualquier otro dispositivo.

El envío de datos de salud en caso de que no se puedan entregar en mano al interesado, debe hacerse por correo ordinario, en sobre opaco y donde el interesado aparezca como destinatario. Incluso en los sobres se puede añadir la palabra "confidencial" para aumentar la seguridad en este sentido, o bien por correo electrónico (autorizado por el trabajador) y de manera cifrada.

Normativa aplicable: Ley 15/1999 de 13 de diciembre de LOPD y RD 1720/2007.

6. Uso del ordenador profesional fuera de la empresa

Siempre que un profesional necesite llevarse documentación fuera de su lugar de trabajo, aunque sea para precisamente eso, trabajar, debe pedir autorización al responsable del fichero y tomar las medidas de seguridad pertinentes para salvaguardar la información.

Hay que tener en cuenta en este sentido la posibilidad de pérdida de documentación en cuyo caso, habría que denunciar la pérdida a la Policía siguiendo los trámites protocolizados en cada empresa.

Otra forma de trasladar datos es llevando el ordenador profesional a un lugar ajeno a él para utilizarlo. En un ordenador corporativo tenemos infinidad de datos confidenciales que deben ser tratados con la máxima cautela. Al conectarse el ordenador a una red wifi del hogar, de un hotel, un ciber café… podemos correr el riesgo de que accedan a nuestro equipo personas

ajenas y que consigan accesos a nuestros datos .Además la probabilidad de infectar nuestro ordenador con algún virus, sería más elevada.
Incluso sin sacar el ordenador de la empresa, se hace necesario bloquear el equipo informático en ausencia del puesto de trabajo.
Normativa aplicable: Ley de LOPD 15/1999 Art. 44 y 46.

7. Uso personal del ordenador profesional

Los equipos informáticos solo deben utilizarse con fines profesionales y la utilización de las aplicaciones informáticas sólo tienen una finalidad profesional. Sólo el personal autorizado, podrá instalar, desinstalar o configurar aplicaciones en los ordenadores. Para instalar cualquier aplicación se necesita una licencia y necesita adecuarse a la Ley vigente.
Los usuarios están obligados a utilizar los antivirus y sus actualizaciones o algún otro sistema de seguridad destinado a la prevención y protección de los Sistemas de Información.
Los profesionales sólo deben limitarse a ejecutar las aplicaciones informáticas para las que estén autorizados.
Normativa aplicable: Ley de LOPD 15/1999 Art. 9.

8. Comentarios de pasillo

Una de las formas más fáciles de atentar contra la protección de datos y de liberar el secreto profesional, son los frecuentes comentarios "de pasillo". En demasiadas ocasiones escuchamos hablar entre compañeros con un tono de voz que nos permite entender de lo que está hablando, sobre trabajadores, sobre tratamientos, sobre diagnósticos… y también sobre datos personales, como la procedencia de algunos de los usuarios, su edad, su situación familiar… El problema de hacer todo este tipo de comentarios en el "pasillo" y con un tono de voz al alcance de todos los oídos, es que estamos invadiendo un peliagudo terreno en cuanto a protección de datos se refiere.
También es frecuente hablar de un paciente delante de otro o atender una llamada de teléfono delante de alguna persona donde se dan datos de algún paciente ya sean personales o relativos a su su proceso asistencial.

9. Derechos del trabajador: Arco

El trabajador tiene los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), que puede ejercer en cualquier momento. La organización tiene la obligación de disponer y regular los procedimientos para el ejercicio de estos derechos por parte de los usuarios.
Habría que responder a los derechos de rectificación, cancelación y oposición en diez días hábiles y al derecho de acceso, en un mes. El silencio administrativo no sería posible en el ejercicio de estos derechos.
Derecho de Rectificación: el interesado pide rectificar alguno de sus datos o episodios incluidos en nuestra base de datos. Sólo puede ser solicitado expresamente por el interesado o su representante legal.
Derecho de Acceso: el trabajador tiene derecho al acceso de sus datos, el tratamiento de que está siendo objeto, el origen de dichos datos y las comunicaciones realizadas o previstas de sus datos.
Derecho de cancelación: La cancelación de los datos de carácter personal, no procederán cuando estos deban ser conservados durante los plazos previstos por la ley, o debido a las relaciones contractuales entre las partes que justifican el tratamiento de los datos.
Derecho de Oposición: el trabajador podrá ejercer este derecho como consecuencia de motivos legítimos y fundados, referidos a su concreta situación personal, que lo justifique, siempre que la Ley no imponga lo contrario.
Normativa aplicable: Ley de LOPD 15/1999, Ley General de Sanidad Art.10.

10. Información a terceros

Se puede llegar a requerir en algún momento, información de un trabajador por parte de una persona no autorizada por él. En estos casos, no se pueden revelar datos ni de carácter personal ni del estado de salud del interesado, salvo previa indicación expresa del responsable del fichero o tratamiento, imperativo legal o mandato judicial. También el interesado, podría dar su consentimiento para ello.
En este punto se encontrarían también los familiares que piden información sobre los trabajadores, así como amigos o conocidos, periodistas o curiosos que preguntan por famosos atendidos en nuestras instalaciones…

Conclusiones

Muy acorde con el decálogo y para que sirva como resumen de todo lo expuesto anteriormente, el Código Internacional de Etica para los Profesionales de la Salud Ocupacional (ICOH 2002)[9], en su artículo 21 especifica que: "Los datos médicos personales y los resultados de las investigaciones médicas deben estar registrados en archivos médicos confidenciales, los cuales deben guardarse en forma segura bajo la responsabilidad del médico o la enfermera de salud ocupacional. El acceso a las fichas o archivos médicos así como su transmisión, divulgación y utilización se rige por las leyes o normas nacionales que existan y por los códigos de ética para los profesionales médicos y de la salud. La información contenida es estos archivos solo podrá utilizarse para los fines de la Salud Ocupacional".

Así pues, para poder prestar unos cuidados de calidad las Unidades Básicas de Salud han de tener en cuenta los derechos y las obligaciones emanadas de la legislación vigente.

Los médicos y enfermeros del trabajo, por su ejercicio profesional, acceden y crean cantidad de datos pertenecientes a la intimidad de los trabajadores, a sus problemas de salud, a sus datos personales…, y por ello, para este colectivo profesional se hace necesaria la puesta en marcha de este decálogo. Respecto a ello, se puede llegar a conseguir la prestación de cuidados de calidad e infundir despreocupación a los trabajadores que acuden a su reconocimiento médico.

En un reconocimiento médico laboral, para el médico del trabajo es imprescindible que el trabajador le proporcione todos los datos posibles relativos a su historial de salud, ya que debe basarse en esos antecedentes y en los resultados de su reconocimiento médico actual, para emitir una aptitud laboral. De ahí la importancia de que el trabajador sea lo más sincero posible en la anamnesis que hace el profesional y resulta necesario también que el trabajador esté familiarizado con este deber de protección de datos para su mayor tranquilidad en este sentido.

Más que a ocultar al médico del trabajo alguna información relevante, el trabajador suele demostrar desconfianza por las posibles filtraciones a la empresa de sus datos de salud, por eso se debe informar de manera clara al trabajador sobre el deber de salvaguardar toda la información que surja fruto de la relación con los profesionales y más concretamente, fruto del reconocimiento médico.

Para poder dar esta información al trabajador y para poder prestar un servicio de calidad, el profesional debe estar familiarizado con todo lo concerniente a la protección de datos, al secreto profesional, a la vulneración de ese secreto, siendo capaz de cumplir el presente el decálogo en su vida laboral. ea lo m a su historia de salud, ador sea lo m De ahesultados de su reconocimiento ms posibles relativos a su historia de salud,

Bibliografía

1. Calvo Sánchez, MD. Enfermería del Trabajo. Serie de cuidados avanzados. En: España. Paradigma; 2008. P. 67-87.

2. Fernández Lamelas MA, Álvarez Rodriguez T, Ramiro Fernández JM, Martínez de Santiago S. El Respeto a la Intimidad. El Secreto Profesional en Enfermería. Cuad Bioét 2008; XIX: 59-66.

3. Plan de Sensibilización en materia de Protección de Datos. (on line). Disponible en: http://www.hvn.es/servicios_noasistenciales/subdireccion_nuevas_tecnologias/ficheros/ideasclaveplansensibilizacionlopd.pdf.Acceso 12/06/2015.

4. Guía: La protección de Datos en las Relaciones Laborales. (on line). Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_RelacionesLaborales2.pdf.Acceso 01/03/2016.

5. Constitución Española. BOE núm. 311, 29 de diciembre de 1978.

6. Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado nº 298 (14-02-1999).

7. Ley 14/1986, de 25 de abril. Ley General de Sanidad. Boletín Oficial del Estado nº 102.

8. Terré Rull C. El Secreto Profesional y la Protección de Datos de Carácter Personal. Matronas Profesión 2002; 9: 36-39.

9. Código Internacional de Ética para los Profesionales de la Salud Ocupacional. (on line). Disponible en http://www.bvsde.paho.org/cursoa_epi/e/lecturas/mod6/codigo.pdf
Acceso 01/03/2016.