

La protección de datos sanitarios: perspectiva ética

The protection of health information: ethical perspective

Constantino González Quintana¹



RESUMEN

INTRODUCCIÓN. La protección de datos personales relacionados con la salud ha sido siempre objeto de la deontología sanitaria desde sus orígenes. Actualmente ya no se trata de una obligación unilateral del profesional sanitario, sino de una exigencia ética y jurídica basada en la protección de los derechos de los pacientes. Los estudios de *Big Data* están introduciendo un giro copernicano que abren la puerta a conocimientos científicos inéditos, mejoras continuas en todas las especialidades sanitarias y, sobre todo, una atención mucho más personalizada. También presentan retos de gran envergadura a los que hay que responder desde el respeto a la dignidad de las personas y a sus derechos fundamentales. Así será posible buscar el equilibrio entre innovación y protección, entre libertad y seguridad.

PALABRAS CLAVE: datos personales relacionados con la salud, *Big Data*, ética, bioética, dignidad humana, respeto a la persona, intimidad personal, protección, confidencialidad.

ABSTRACT

INTRODUCCIÓN. The protection of data personal related with the health has been always object of the ethics health since its origins. Currently it is not a unilateral obligation of the sanitary one, but of an ethical and juridical exigency based on the protection of the Rights of the patients. Big Data's studies are introducing a Copernican draft that open the door to knowledge scientific unpublished, improvements continuous in all them specialties health and, above all, an much more personalized attention. Also they presented challenges of great importance to which it is necessary to answer from the respect to the dignity of the persons and to his fundamental rights. This way it will be possible to look for the balance between innovation and protection, between freedom and safety.

PALABRAS CLAVE: Personal data related to health, Big Data, ethics, bioethics, human dignity, respect for the person, personal privacy, protection and confidentiality.

¹ Titular del Blog Académico: Bioética desde Asturias. España

Correspondencia: Dr. Constantino González Quintana. Titular del Blog Académico: Bioética desde Asturias. Oviedo. Asturias. España.
Correo electrónico: constantinoq147@gmail.com .

El origen vivo y directo de la ética médica, y de las profesiones sanitarias, reside en la relación clínico-asistencial y en el contenido de esa relación, es decir, en el fin interno que define a la práctica sanitaria y le confiere sentido ético y legitimidad social. Ahí es donde los profesionales sanitarios construyen su identidad ética, porque decir “yo” significa “heme aquí”, que equivale a vivir actuando para el bien de sus pacientes.

La bioética clínica (del griego *klíne*, “cama”) no es más que la ética de las relaciones clínico-asistenciales, es decir, la práctica sanitaria aprendida y ejercida junto a la cama de los pacientes, cuyo centro es la confianza entre la persona enferma y el profesional sanitario. Consiste en adquirir valores éticos y positivizarlos cada día, cumplir deberes u obligaciones (principios y reglas), asumir buenas disposiciones o “virtudes”, y tomar buenas decisiones practicando la deliberación¹.

1. Datos personales relacionados con la salud

Parece pertinente comenzar exponiendo los conceptos básicos que vamos a manejar a lo largo de estas páginas, tomando como referencia el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal².

- a) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
- b) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
- c) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Los datos sanitarios surgen, en primera instancia, de la relación clínico-asistencial, donde, la persona

enferma, basándose en el valor ético de la confianza, expone libremente al profesional sanitario su intimidad, iniciándose así el proceso de recogida, acumulación, archivo y tratamiento de datos personales relacionados con la salud. Son datos especialmente sensibles y objeto de derechos de “carácter personalísimo”.

Este tipo de datos están contenidos, básicamente, en la historia clínica, pero también en la receta médica, en los documentos de instrucciones previas y en la tarjeta sanitaria individual. La utilización, archivo, custodia y transmisión de estos datos, pone en juego la legalidad vigente y, además, sirve para medir la estatura moral de cada uno, sea éste individuo, equipo, hospital, sistema sanitario o empresa farmacéutica.

Conviene recordar, a ese propósito, que la persona enferma es mucho más que la suma de sus datos sanitarios. No son informes neurológicos o bioquímicos que se puedan mirar “con la pupila quieta”, como decía Ortega y Gasset³. Hacerlo así supondría congelar a la persona en cifras y convertirla en una foto fija. La medicina necesita datos basados en evidencias, pero esos datos narran una biografía personal y están supeditados al bien de esa persona que tiene primacía respecto al interés de la ciencia o la sociedad. Reducirlo todo a números implica deshumanizar la atención sanitaria.

2. El desafío de los *big data* sanitarios

En términos muy generales entendemos por *Big Data* aquel conjunto de datos que, por su tamaño ingente, sobrepasa la capacidad de ser gestionado por bases de datos de integración tradicionales. Hay un gran acuerdo en afirmar que se fundamenta en el paradigma de las tres “V” (volumen, variedad y velocidad): el elevadísimo “volumen” de datos que precisa nuevas técnicas de almacenamiento y enfoques distintos para recuperar y manejar la información; la “variedad” de las fuentes de datos (texto, audio, vídeo, etc.) que hace que las redes relacionales sencillas sean difícilmente aplicables; y, por último, el incesante incremento con que se generan los datos hace que la “velocidad” sea un parámetro clave en su manejo. Hay quienes añaden la V referente al “valor” aportado por estos grandes conjuntos de datos, así como la V de “veracidad” que determina el grado de confianza o fiabilidad que merecen los datos a la hora de tomar decisiones.

Es admitido hoy por todos que los estudios de *Big Data* en el ámbito sanitario representan una especie

de giro copernicano en el sentido de que ya está abriendo la puerta a conocimientos científicos inéditos, mejorará las prestaciones de todas las especialidades sanitarias y, sobre todo, hará mucho más personalizada la actividad asistencial.⁴

Junto a las enormes posibilidades y aplicaciones de *Big Data* parece de suyo evidente que es necesario incrementar las medidas de protección de las personas. El propio creador de *Facebook* aseguraba hace algunos años que las personas deben ser conscientes de que “compartir los datos les pone en una situación de vulnerabilidad”. En el ámbito sanitario, el uso de *Big Data* va a depender tanto de la educación como de la constante actualización de normas jurídicas. Pero, además, deberá estar basado en un imperativo moral, dado que el sentido ético y la correspondiente legitimidad social de cualquier sistema sanitario proceden específicamente de una finalidad ética: curar y cuidar la salud y la vida⁵. Se trata, en suma, de articular medidas educativas, jurídicas y, en nuestro caso, éticas, para garantizar la innovación en la mejora de la salud y, al mismo tiempo, proteger los derechos de las personas, o sea, equilibrar libertad y seguridad.

La puesta en valor de los *Big Data* en orden al desarrollo de la biomedicina y del bienestar social queda en entredicho cuando se comprueba que los criterios de disociación y anonimización de los datos personales pueden estar quedando superados u obsoletos. Así parece haber sucedido cruzando una base de datos anonimizada con una base de datos de los votantes de un Estado norteamericano (código postal, fecha de nacimiento, dirección, sexo). Muchos de esos datos fueron “desanonimizados” y fue posible identificar nominalmente a las personas⁶. En el fondo de todo ello queda cuestionada la validez del tratamiento e intercambio de datos sensibles y, sobre todo, quedan bajo sospecha la misma protección de datos, la intimidad personal, la confidencialidad, el secreto profesional y el propio concepto de “datos personales”.

Por eso es tan decisivo el compromiso de la gobernanza para gestionar estos datos, que corresponde a las autoridades públicas como garantes de los derechos fundamentales. En este sentido, el Nuffield Council on Bioethics recomienda los siguientes principios⁷: 1) respeto a las personas; 2) respeto de los derechos humanos; 3) participación de las personas con intereses moralmente relevantes; y 4) responsabilidad de las decisiones.

Y por eso es tan importante el requisito de la legitimación como: 1º) legitimación legal o justificación

del tratamiento de datos por razones de interés público (atención sanitaria, calidad y gestión del servicio y fines científicos: epidemiológicos, investigación, docencia); y 2º) legitimación voluntaria o consentimiento expreso de la persona para el tratamiento de datos con fines exclusivamente privados o distintos de los de su origen (industria, farmacia, biotecnología).

El requisito de la legitimación permite el acceso de terceros a los datos y, a la vez, pone en manos de sus titulares el control sobre su información personal.

Hay otros retos éticos que conlleva la aplicación del análisis de los *Big Data* referentes a la salud pública, al apoyo de la decisión clínica, a la gestión sanitaria, a las compañías de seguros y las prescripciones de fármacos. No es posible abordarlos aquí.

4. Bases éticas de la protección de datos sanitarios

Incluso con independencia de la posición que pueda tener cada uno respecto al humanismo médico y la humanización de la asistencia, hoy día está colectivamente asumida la obligación de respetar incondicionalmente la dignidad humana como centro sobre el que gira toda la bioética⁸, porque el ser humano es absolutamente valioso para el propio ser humano. La exigencia de no instrumentalizar a la persona se traduce en la primacía que se le debe otorgar a todos los efectos, por encima de los intereses de la ciencia, la sociedad, los hospitales y las empresas dedicadas al archivo, estudio y explotación de los datos personales relacionados con la salud.

4.1. Valores éticos referentes a la protección de datos sanitarios

La dignidad humana: Es el valor intrínseco e inherente de todo ser humano. No se refiere a algo sino a alguien que no tiene equivalente, porque es único e irremplazable. Por eso debe ser tratado siempre como un fin en sí y nunca como un simple medio para satisfacer intereses ajenos. Es el valor ético sobre el que se fundamentan el resto de valores y principios de actuación.

La libertad humana: Es la capacidad del ser humano para actuar de una manera o de otra, o de no actuar, sin coacciones externas ni internas. El correlato de la libertad es la responsabilidad por la que cada uno se hace cargo de las consecuencias de sus actos.

La intimidad personal: Es lo más interior y reservado, propio y exclusivo de la persona, accesible sólo

a ella y que sólo ella decide compartir con otros. Su función es proteger frente a cualquier invasión que pueda realizarse en el ámbito personal o familiar.

Hay que tener en cuenta, sin embargo, que no hay valores absolutos. Los valores éticos suelen entrar en colisión con otros valores éticos de igual rango en virtud de las circunstancias que concurren en una determinada situación. El valor de la intimidad puede ceder o dejar de obligar cuando aparecen enfermedades de declaración obligatoria que conllevan un grave perjuicio a uno mismo o a terceras personas. Es un ejemplo, entre otros, que ilustra un principio clásico, el principio de excepción, que consiste en la obligación de no aplicar una norma cuando se sabe que de su aplicación se derivan graves consecuencias negativas para la dignidad de las personas como valor fundamental.

4.2. Principios éticos en orden a proteger los datos sanitarios

Protección: Es la obligación moral de amparar, favorecer, defender y resguardar a cualquier ser humano de un perjuicio o peligro que atente contra su dignidad y sus derechos fundamentales como sucede, en este caso, con los datos sanitarios.

Confidencialidad: Es el deber de no divulgar la información personal de salud que pertenece a la intimidad de la vida de una persona. Está recogido en el deber de secreto profesional que garantiza el valor y el derecho a la intimidad.

Limitación de la finalidad: es la obligación de recoger y tratar estos datos sólo para los objetivos específicos y legítimos que se hayan prefijado. Cuando se destinan a otros fines es imprescindible legitimarlo con un consentimiento voluntario y específico.

Los tres principios éticos anteriores se fundamentan en la materia que tratan (dignidad, libertad e intimidad) y en los principios que los justifican: no hacer daño a nadie (no maleficencia) y tratar a todos con la misma consideración y respeto (justicia).

4.3. Reglas para proteger la calidad de los datos sanitarios

1) Tratar los datos de forma leal y lícita; 2) recogerlos y utilizarlos sólo para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento; 3) deben ser adecuados, pertinentes y no excesivos en relación con las finalidades previstas; 4) serán exactos y puestos al día de forma que respondan con veracidad a la situación

actual del afectado; 5) serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad prefijada; 6) serán tratados de forma que permitan el ejercicio del derecho de acceso, rectificación y oposición en tanto no proceda su cancelación; 7) serán siempre objeto de codificación numérica o anonimización en el ámbito de investigación biomédica; y 8) serán excepcionalmente revelados en los casos previstos por la ley.

4.4. Virtudes morales para intensificar la protección de datos sanitarios

Lealtad: Es la disposición positiva de cumplir con aquello que exigen los valores de la dignidad y la intimidad de las personas. La exposición de la intimidad del paciente y la información sobre su salud es objeto de especial lealtad, concretada en la anonimización y la legitimación de los datos.

Veracidad: Es la disposición positiva de buscar y decir la verdad, que está íntimamente relacionado con la disposición de ser sincero, honesto, franco y actuar de buena fe. Es lo opuesto a la mentira y a la falsedad, tan importantes a la hora de proteger datos personales relacionados con la salud.

Honestidad: Es la disposición positiva de comportarse y expresarse con sinceridad y coherencia, respetando los valores de la intimidad y la verdad. Consiste en respetarse a sí mismo y a los demás. Es una pieza clave de las relaciones humanas y, en particular, de las de confianza sanitario-paciente, tanto para guardar secreto como para revelarlo de manera proporcionada y en sus justos límites, basados en el principio de excepción.

4.5. Deber moral de respetar los derechos referentes a la protección de datos

El reciente Reglamento de la Unión Europea sobre la materia recoge los siguientes derechos⁹: 1) transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado; 2) información y acceso a los datos personales; 3) información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado; 4) derecho de acceso del interesado; 5) derecho de rectificación; 6) derecho de supresión (“el derecho al olvido”); 7) derecho a la limitación del tratamiento; 8) obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento; 9) derecho a la portabilidad



de los datos; 10) derecho de oposición; 11) decisiones individuales automatizadas, incluida la elaboración de perfiles.

Hoy es bien sabido por todos que, en Hacienda, en los Hospitales, en *Google*, en *Facebook* y en *Whats App*, saben de nosotros mucho más que nosotros mismos. Vivimos “la creciente y desazonadora certeza de estar en un mundo cada vez más informatizado donde todo se vigila, tanto lo grande como lo pequeño, y donde lo que reporta beneficios siempre termina siendo una fuente de explotación”¹⁰. De ahí que no sea ninguna pedantería lingüística solicitar el empoderamiento progresivo de los ciudadanos si no queremos vivir cada vez más tutelados y manipulados por el ojo del “gran hermano global”.

Por eso es necesario poner de relieve que la utilidad de los algoritmos computerizados, para extraer de las bases de datos nueva información y nuevos puntos de vista, son una gran ayuda para tomar decisiones clínicas, pero nunca sustituyen la responsabilidad del profesional ni eliminan la incertidumbre propia de su decisión. El razonamiento médico ha de tener en cuenta los valores, las necesidades y las prioridades de los enfermos concretos. Y esto no es una habilidad computable ni estadística. Es una habilidad ética que se debe aprender todos los días.

Referencias

1. González Quintana C. Bioética médica: fundamentos mínimos (I) (y II). (acceso: 2017-16-01). Disponible en: <http://www.bioeticadesdeasturias.com/2015/01/bioetica-medica-i-fundamentos-minimos.html> y en <http://www.bioetica-desdeasturias.com/2015/01/bioetica-medica-i-fundamentos-minimos.html>.
2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (acceso: 17-01-2017). Disponible en: <https://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf>.
3. Ortega y Gasset J. Obras completas. IX. Madrid: Taurus; 2004-2020. p 1266.
4. Rock Health. Big Data in digital Health. (acceso: 18-01-2017). Disponible en: <http://www.slideshare.net/RockHealth/rock-report-big-data>.
5. Llàcer MR, Casado M, Buisán L (coords.). Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública. Barcelona. (acceso: 21/01/2017). Disponible en: <http://www.publicacions.ub.edu/refs/observatoriBioEticaDret/documents/08209.pdf>.
6. León Sanz P. Bioética y explotación de grandes conjuntos de datos. En: Carnicero Jiménez J, Rojas de la Escalera D (coords.). La explotación de datos de salud. Retos, oportunidades y límites. Madrid: Sociedad Española de la Informática de la Salud; 2016. p. 30. (acceso 23/01/2017). Disponible en: <http://www.seis.es/documentos/Informe%20La%20explotacion%20de%20datos%20de%20Salud/LA%20EXPLORACION%20DE%20DATOS%20DE%20SALUD.pdf>.
7. The collection, Linking and Use of Data in Biomedical Research and Health care: Ethical Issues. 2015. p. 84.153-156. (acceso: 22/01/2017). Disponible en: http://nuffieldbioethics.org/wpcontent/uploads/Biological_and_health_data_web.pdf.
8. UNESCO. Declaración sobre bioética y derechos humanos. 2005. Arts. 3.1-2. (acceso: 19/01/2017). Disponible en: <http://unesdoc.unesco.org/images/0014/001461/146180s.pdf>.
9. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Arts. 12-22. (acceso: 19/01/2017). Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>.
10. Larsson S. Millennium 4. Lagercrantz D. Lo que no te mata te hace más fuerte. Barcelona: Círculo de Lectores; 2015. p. 635-636.