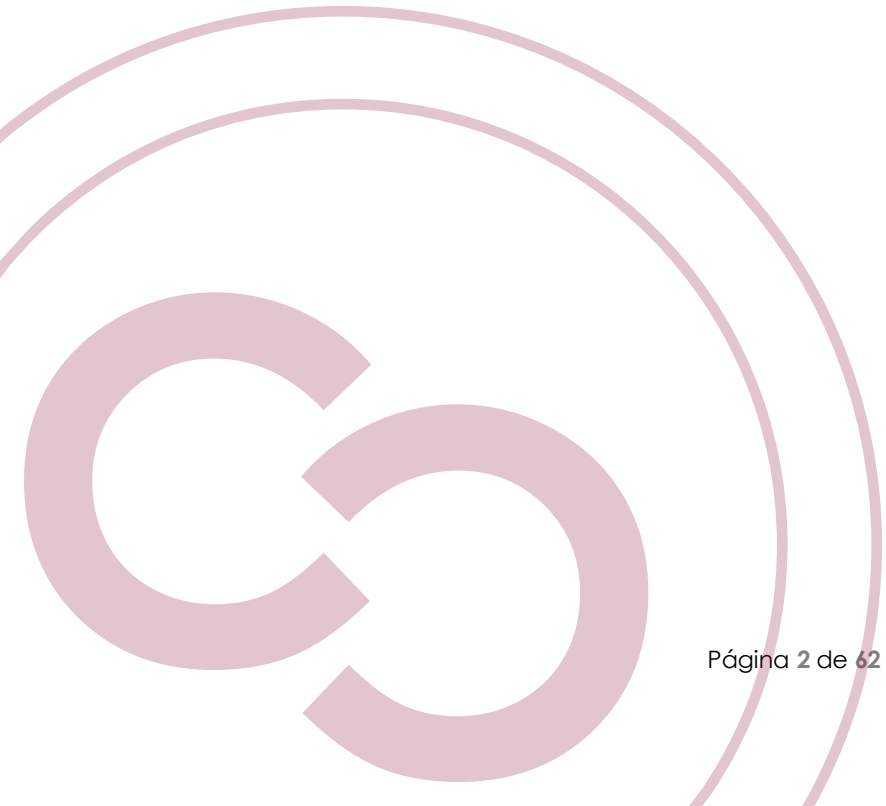
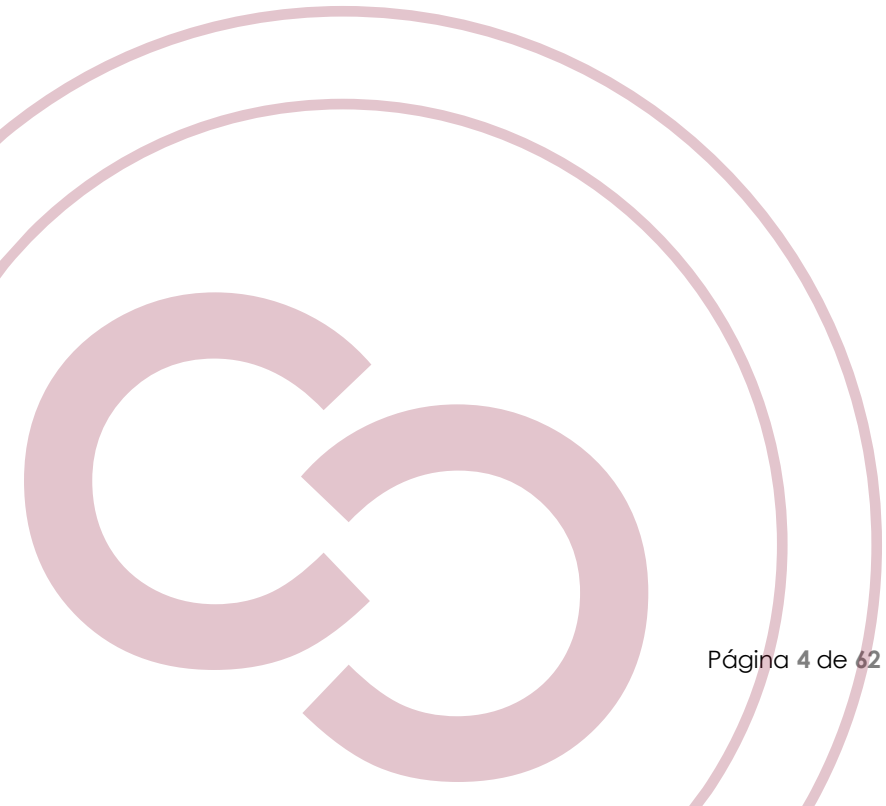
Código de Conducta para el tratamiento de datos personales en el ámbito sanitario

Consorcio de Salud y Social de Cataluña

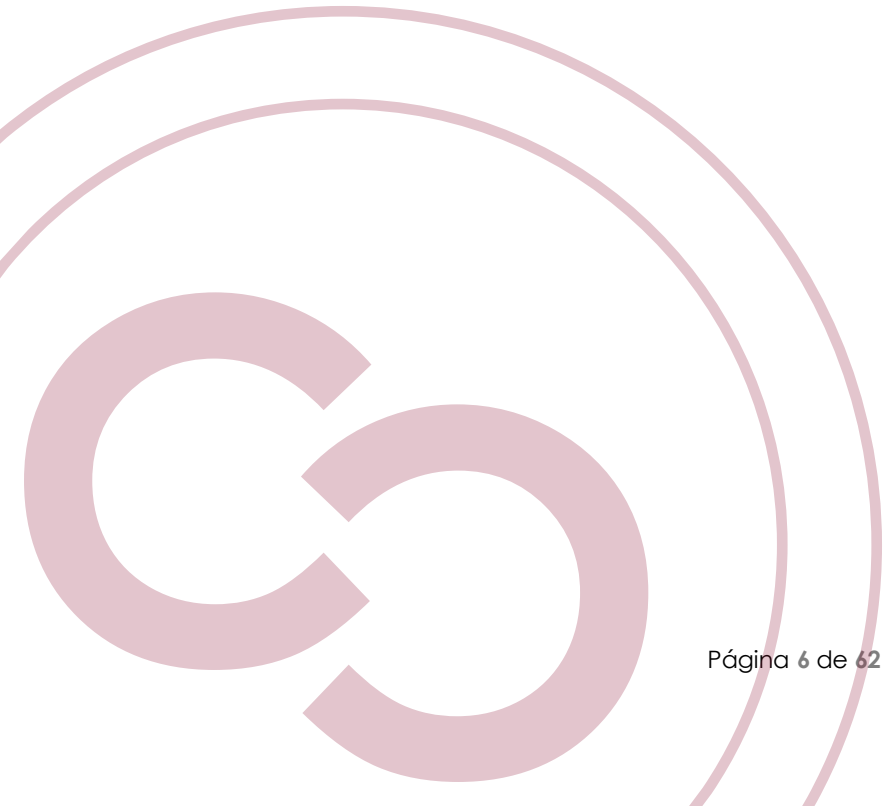
Codi de Conducta
Consorci de Salut i Social de Catalunya



Índice



Libro primero



Índice

Libro primero. Disposiciones generales

Título I - Ámbito y régimen de aplicación

Capítulo I - Normativa aplicable

Artículo 111-1. Marco normativo de referencia

1. El presente Código de Conducta tiene como marco de referencia la normativa en materia de protección de datos personales, así como las especialidades en la aplicación de esta normativa en el ámbito sanitario.

   En este sentido, se toma en consideración la normativa en materia de protección de datos personales y la normativa sectorial de aplicación a las entidades del ámbito sanitario sobre el tratamiento de datos personales.

2. La normativa en materia de protección de datos personales que este Código de Conducta ha adoptado como marco de referencia es la que se detalla a continuación:

   a. 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 relación con el 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).
   b. Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
   c. 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, en lo que no se oponga al Reglamento general de protección de datos y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

3. La normativa sectorial de aplicación a las entidades de ámbito sanitario es la que se detalla a continuación:

   a. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y del derecho y obligaciones en materia de información.
   b. Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica.
   c. Ley 14/1986, de 25 de abril, General de Sanidad.
   d. Ley 44/2003, de 21 de noviembre, de ordenación de profesiones sanitarias.
   e. Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
   f. Ley 14/2007, de 3 de julio, de Investigación biomédica.
   g. Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales.
   h. Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, el Comité de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos.
   i. Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se

aprueba el protocolo mediante el cual se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente para los alumnos y residentes en Ciencias de la Salud.

j. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.
k. Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y de Atención a las personas en situación de dependencia.
l. Ley 12/2007, de 11 de octubre, de Servicios Sociales.

4. El cumplimiento de las disposiciones previstas en el presente Código de Conducta no exime del cumplimiento de la normativa en materia de protección de datos personales vigente en cada momento. Las entidades adheridas al presente Código se comprometen a seguir la normativa vigente aplicable en cada momento en materia de protección de datos.

5. La normativa aplicable en materia de protección de datos y las disposiciones del presente Código tienen carácter mínimo. Las disposiciones tanto de la normativa aplicable como del Código pueden ser complementadas por los responsables y encargados del tratamiento.

Capítulo II - Ámbito de aplicación

Artículo 112-1. Ámbito objetivo de aplicación

La misión que tiene encomendada este Código de Conducta es la creación de un marco común y la unificación de criterios en la aplicación de la normativa de protección de datos personales en el sector sanitario.

El presente Código de Conducta tiene por objeto establecer las medidas y actuaciones que deben seguir los responsables del tratamiento o encargados del tratamiento en el marco de las actividades asistenciales, médicas o de investigación en salud. Asimismo, se pretende ofrecer soluciones a situaciones complejas en la aplicación de esta normativa dentro del sector.

Artículo 112-2. Ámbito subjetivo de aplicación

1. El presente Código de Conducta será de aplicación para todos aquellos tratamientos efectuados por las entidades adheridas que pertenezcan al sector de la atención sanitaria, que formen parte del ámbito competencial de la Autoridad Catalana de Protección de Datos y manifiesten expresamente su voluntad de adherirse a este Código de Conducta, con independencia de que sean entidades asociadas al Consorcio de Salud y de Atención Social de Cataluña.

2. El presente Código de Conducta será de aplicación para los tratamientos de datos efectuados por las entidades que, aunque no pertenezcan al sector sanitario, presten servicios, como encargadas del tratamiento a las entidades indicadas en el apartado anterior y que manifiesten su voluntad de adherirse a este Código de Conducta. Las disposiciones del presente Código serán aplicables a los tratamientos que se deriven de estos encargos de tratamiento.

Artículo 112-3. Entidades a las que va dirigido el Código de Conducta

1. Los centros hospitalarios de titularidad pública o privada adscritos al sistema sanitario integral de utilización pública de Cataluña (SISCAT), que hayan mostrado interés en adherirse al presente Código y una vez aprobada la adhesión.

2. Los centros sanitarios que presten servicios de atención primaria, ambulatoria o domiciliaria, de titularidad pública o privada, adscritos al sistema sanitario integral de utilización pública de Cataluña (SISCAT), que hayan mostrado interés en adherirse al presente Código y una vez aprobada la adhesión.

3. Los centros sanitarios cuyo objeto sea hacer pruebas de carácter médico, de diagnóstico de la imagen, de análisis químico o cualquier otro servicio diagnóstico que presten servicios a otras entidades de titularidad pública o privada adscritas al sistema sanitario integral de utilización pública de Cataluña (SISCAT), que hayan mostrado interés en adherirse al presente Código y una vez aprobada la adhesión.

4. Entidades que presten servicios de salud laboral y vigilancia de la salud a otras entidades de titularidad pública o privada adscritas al sistema sanitario integral de utilización pública de Cataluña (SISCAT), de manera exclusiva o no, que elaboren o mantengan historias clínicas al efecto, que hayan mostrado interés en adherirse al presente Código y una vez aprobada la adhesión.

5. Entidades de carácter científico o técnico que hagan tareas de investigación, desarrollo, investigación, docencia o formación en el ámbito sanitario, sin perjuicio de la disciplina científica, médica o tecnológica en que se desarrolle, siempre que tenga relación con metodologías de tipo asistencial , de diagnóstico médico, de tratamiento de la salud y cuidado, prevención o paliación de los efectos de las enfermedades y procesos patológicos o episodios relacionados con la salud mental, así como el estudio y optimización de los procedimientos y recursos relacionados con la atención al enfermo, incluyendo estudios observacionales y estadísticos y sistemas de inteligencia artificial aplicados al ámbito asistencial o sanitario, que presten servicios a otras entidades adscritas al sistema sanitario integral de utilización pública de Cataluña (SISCAT), de manera exclusiva o no, o dependan orgánicamente o funcionalmente de una de estas entidades, que hayan mostrado interés en adherirse al presente Código y una vez aprobada la adhesión.

6. El ámbito de aplicación definido en el apartado 1 no impedirá la aplicación del presente Código a las otras entidades que soliciten la adhesión cuando su sector de actividad tenga una relación o vinculación manifiesta con el sector sanitario. En estos casos la petición de admisión deberá motivar esta relación o vinculación

y el Órgano de Supervisión deberá emitir una valoración de la adecuación de la admisión de carácter vinculante.

7. El presente libro será de aplicación a las entidades que presten servicios auxiliares a entidades, adscritas al sistema sanitario integral de utilización pública de Cataluña (SISCAT), de manera exclusiva o no, o dependan orgánicamente o funcionalmente de una de estas entidades , que hayan mostrado interés en adherirse al presente Código y una vez aprobada la adhesión. Entre los servicios auxiliares mencionados se pueden incluir los servicios logísticos, de almacenamiento de información, de prestaciones de carácter técnico o informático.

8. A los efectos del punto anterior, las entidades prestadoras de servicios auxiliares podrán asumir la adopción del presente Código para servicios concretos. Corresponderá a la entidad identificar correctamente los servicios ofrecidos que impliquen tratar los datos personales en cuestión de acuerdo con las disposiciones del presente Código. El promotor del presente Código indicará, en cumplimiento del deber de publicación de las entidades adheridas, los servicios concretos que se regulan por el presente Código.

9. Podrán adherirse al presente Código de Conducta las entidades que, sin corresponderse con las anteriormente mencionadas, actúen de manera habitual como encargadas del tratamiento de otras entidades adheridas, de acuerdo con lo dispuesto en el artículo 112-2.2 del presente código.

Título II - Adhesión al Código de Conducta

Capítulo I - Adhesión al presente Código de Conducta

Artículo 121-1. Procedimiento de adhesión al Código de Conducta

Toda entidad que tenga la voluntad de adherirse al presente Código de Conducta deberá comunicarlo por escrito al Consorcio de Salud y de Atención Social de Cataluña, mediante la solicitud de adhesión del Anexo 1, que deberá incluir de manera expresa la voluntad de adherirse y la identificación como organización que trata datos en el ámbito de los servicios de la salud.

La solicitud será remitida al Órgano de Supervisión del Código de Conducta, que revisará y analizará el grado de cumplimiento del solicitante de acuerdo con la documentación que se le pueda requerir. Mediante la entrega de la solicitud de adhesión, con la que comienza el procedimiento de adhesión, las entidades manifiestan así la voluntad de dar cumplimiento a la normativa aplicable en protección de datos, así como a las disposiciones contenidas en el presente Código .

El Órgano de Supervisión dictará de forma motivada la resolución expresa en el plazo máximo de un mes, desde la recepción de toda la documentación adicional que se requiera, aceptando o no la adhesión del solicitante a este Código de Conducta.

El Órgano de Supervisión tendrá en cuenta el grado de cumplimiento de la normativa en materia de protección de datos y de las disposiciones de este Código de Conducta para resolver la solicitud de adhesión, así como la formación en esta materia del personal de la entidad solicitante.

La condición de entidad adherida al Código de Conducta tendrá carácter permanente, con renovación anual y hasta que se den las circunstancias previstas para la pérdida de la condición de entidad adherida al Código de Conducta.

Artículo 121-2. Resolución del Órgano de Supervisión a la solicitud de adhesión

En caso de que el Órgano de Supervisión rechace la solicitud de adhesión a una entidad, se dará un plazo de un mes para que ésta pueda hacer enmiendas a la solicitud. En caso de que la entidad solicitante realice las enmiendas correspondientes, el Órgano de Supervisión dispondrá del plazo de un mes para validar la adhesión al presente Código de Conducta.

Si transcurrido el plazo de un mes, la entidad solicitante no ha hecho las correspondientes enmiendas, el Órgano de Supervisión denegará de forma motivada la solicitud de adhesión, sin perjuicio de que esta entidad pueda pedir otra solicitud de adhesión posteriormente.

Artículo 121-3. Aplicación del Código de Conducta a los encargados de tratamiento

1. Las disposiciones previstas en el presente Código de Conducta serán aplicables a las entidades adheridas de conformidad con lo dispuesto en los artículos anteriores cuando actúen como encargadas del tratamiento por cuenta de un tercero responsable.

2. La adhesión al presente Código de Conducta de una entidad del sector sanitario que actúe como encargada del tratamiento por otra entidad del sector sanitario será valorada positivamente por el responsable del tratamiento. Esta adhesión se valorará como elemento que acredite que el encargado del tratamiento presenta suficientes garantías en la aplicación de medidas técnicas y organizativas apropiadas para el tratamiento de los datos.

3. Las entidades adheridas a este Código de Conducta podrán, cuando hagan encargos de tratamiento a entidades que no formen parte del ámbito sanitario, recoger el compromiso del potencial encargado del tratamiento de adherirse al presente Código de Conducta una vez formalizado este encargo . Este hecho se tendrá en cuenta a efectos de considerar que el encargado del tratamiento presenta garantías suficientes para el tratamiento de los datos personales de manera adecuada.

4. La adhesión al presente Código de Conducta de una entidad que preste servicios de tratamiento de datos como Encargada del Tratamiento se considerará un elemento para valorar la elegibilidad como encargado del tratamiento, de acuerdo con las garantías en la aplicación de medidas técnicas y organizativas adecuadas

y en la protección de los derechos de los interesados, de conformidad con lo dispuesto en el artículo 28.1 del Reglamento general de protección de datos.

5. Sin perjuicio de lo dispuesto en los apartados anteriores, todo encargo de tratamiento deberá prever mecanismos que aseguren el cumplimiento de la seguridad del tratamiento en los términos establecidos en los artículos 28 y 32 del Reglamento general de protección de datos.

6. En relación con la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, cuando las medidas aplicadas por el responsable del tratamiento se correspondan con las previstas en el Esquema Nacional de Seguridad por razón de su inclusión entre las entidades recogidas en el artículo 77.1 de la misma ley o por razón de la naturaleza del tratamiento de los datos por la administración pública de origen, será necesario establecer, para el encargado del tratamiento, la obligación de adoptar las medidas de seguridad equivalentes o análogas a aquellas previstas en el Esquema Nacional de Seguridad para el responsable del tratamiento o para la administración pública de origen.

Artículo 121-4. Registro y lista de entidades adheridas

La adhesión dará lugar a la inscripción de la entidad en la lista de entidades adheridas que aparecerá en la página web del Consorcio de Salud y de Atención Social de Cataluña. Además, el hecho de recibir la consideración de entidad adherida conllevará la entrega de un certificado y un distintivo que acredita el cumplimiento de las condiciones estipuladas para formar parte del presente Código. Tanto el certificado como el distintivo podrán ser utilizados por la entidad para acreditar el grado de cumplimiento de la normativa en materia de protección de datos en el ámbito sanitario frente a terceros.

Artículo 121-5. Procedimiento de renuncia a la condición de entidad adherida

1. Las entidades adheridas al presente Código podrán, en cualquier momento, revocar la voluntad de adhesión al presente Código, así como solicitar la retirada de su condición de entidad adherida al Código. Para solicitar esta renuncia, deberán rellenar el formulario contenido en el Anexo 2 y remitirlo al Órgano de Supervisión por medios electrónicos para activar el procedimiento de salida de la entidad.

   La salida será efectiva en el plazo máximo de tres meses desde la solicitud de baja como entidad adherida al Código de Conducta y siempre que no se encuentre abierto un expediente respecto de eventuales incumplimientos de la entidad solicitante. La renuncia a la condición de entidad adherida comportará a la vez la salida de la lista de entidades adheridas publicada en la página web del Consorcio de Salud y de Atención Social de Cataluña, así como el regreso del distintivo entregado previamente a la entidad para acreditar el cumplimiento frente a terceros.

2. Una vez finalizado el procedimiento de renuncia, la entidad que haya perdido la condición de entidad adherida podrá, en cualquier momento, volver a presentar la

solicitud de adhesión siguiendo el procedimiento de adhesión al Código de Conducta establecido en el artículo 121-1.

Capítulo II - Identificación de la entidad como adherida al presente Código de Conducta

Artículo 122-1. - Denominación de la entidad adherida

Las entidades sujetas a las obligaciones derivadas del presente Código de Conducta por motivo de su adhesión pueden utilizar la denominación "entidad adherida al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña ".

Artículo 122-2. - Identificación transitoria

Las entidades que hayan manifestado la voluntad de adherirse al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña podrán indicar o hacer mención al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña añadiendo la indicación "entidad en trámite de adhesión", "entidad pendiente de aprobación" o cualquier otra expresión que manifieste de manera clara el hecho de que la entidad aún no se encuentra formalmente sujeta a las obligaciones del presente Código.

Artículo 122-3. - Identificación inadecuada como entidad adherida

1. La identificación ilegítima de una entidad como entidad adherida al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña o expresiones equivalentes que conduzcan a error sobre la adhesión o sujeción de la entidad al Código de Conducta implicará, sin perjuicio de las acciones correspondientes, la imposibilidad de la entidad de adherirse al Código de Conducta por un plazo de dos años.

2. Las previsiones previstas en el apartado anterior serán también aplicables a las entidades que se encuentren en la situación prevista en el artículo 122-2 del presente Código y que no hagan mención a que la adhesión se encuentra pendiente de resolución.

3. Las entidades que, habiendo iniciado el procedimiento de adhesión, no corrijan, a requerimiento del Órgano de Supervisión, la identificación inadecuada o conducente a error a la que se refiere el artículo anterior, verán suspendido el procedimiento de adhesión al Código de Conducta, y deberán iniciar un nuevo procedimiento de adhesión en el plazo mínimo de seis meses desde la suspensión del procedimiento de adhesión.

Título III - Mecanismos de control del cumplimiento de este Código de Conducta

Capítulo I - Órgano de Supervisión

Artículo 131-1. Órgano de Supervisión

1. El Consorcio de Salud y de Atención Social de Cataluña constituirá un Órgano de Supervisión de este Código de Conducta que funcionará de manera colegiada y estará integrado por expertos en materia de protección de datos personales con experiencia demostrada en el sector sanitario.

2. El Órgano de Supervisión estará formado por un mínimo de tres personas, aunque podrá ampliarse a los efectos de poder asumir con garantías las competencias reservadas al órgano.

3. Se podrán crear listas de miembros suplentes a los efectos de cubrir las plazas que puedan quedar vacantes fruto de recusaciones u otras causas justificadas que impidan a algún miembro ejercer sus funciones. En caso de sustitución, el sustituto se escogerá de entre las personas de la lista de suplentes por sorteo.

Artículo 131-2. Funciones del Órgano de Supervisión

Las funciones del Órgano de Supervisión son:

a. Promover e informar sobre el contenido de este Código de Conducta, los procedimientos de adhesión y de garantía de cumplimiento a las entidades que desarrollen su labor en el ámbito sanitario.
b. Evaluar el grado de cumplimiento del presente Código de Conducta y aplicar el régimen sancionador previsto en este Código.
c. Revisar el contenido de este Código de Conducta con una periodicidad anual, o cuando haya cambios legislativos, tecnológicos o de otro tipo que lo justifiquen.
d. Resolver las solicitudes de adhesión.

Artículo 131-3. Requisitos de los miembros del Órgano de Supervisión

1. Los miembros del Órgano de Supervisión sólo podrán ser designados cuando cumplan con los siguientes requisitos:

   a. Tener los conocimientos necesarios en Derecho y una práctica demostrada en la aplicación de la normativa de protección de datos.
   b. Asumir el compromiso de actuar con independencia e imparcialidad en relación con las entidades adheridas.
   c. Actuar de forma en que no se pueda dar una situación de conflicto de intereses. En caso de que alguna situación cree un conflicto de intereses deberá prever un mecanismo por el que la persona afectada por el conflicto de intereses quede apartada de la toma de decisiones.

d. Cumplir con los deberes y obligaciones establecidos en el Estatuto de los miembros del Órgano de Supervisión.
e. Suscribir un código ético, aprobado por el mismo órgano, que incluya la obligación de poner en conocimiento de este cualquier situación de conflicto de intereses o falta de independencia, autonomía o imparcialidad, para apartarse de manera voluntaria de cualquier decisión o deliberación que pueda verse viciada por estas causas.

2. La experiencia y pericia de los miembros del Órgano de Supervisión se valorará, entre otros, en virtud de los siguientes elementos:

a. La trayectoria profesional.
b. Las certificaciones voluntarias a las que hace referencia el artículo 35 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.
c. Títulos y certificaciones que acrediten conocimientos específicos en protección de datos.
d. Certificaciones en el ámbito de la protección de datos y en el ámbito del presente Código de Conducta.

Artículo 131-4. Evaluación y formación continuada de los miembros del Órgano de Supervisión

1. El Órgano de Supervisión procurará a sus miembros la formación necesaria para el correcto desarrollo de sus funciones y para garantizar el mantenimiento de las condiciones adecuadas.

2. Se publicará, de forma anual, la lista de miembros del Órgano de Supervisión, junto con el currículum de cada uno, así como las titulaciones y certificaciones que procedan.

3. La información de los miembros suplentes se publicará desde el momento en que desarrollen tareas como miembros del Órgano de Supervisión.

4. Se publicará, anualmente, una memoria en la que se indiquen las actuaciones de los miembros del Órgano de Supervisión, así como las formaciones, certificaciones o títulos alcanzados durante el año.

5. Las listas a las que se refieren los apartados anteriores deberán estar disponibles durante el tiempo de ejercicio del cargo de los miembros del Órgano de Supervisión. A los efectos de disponibilidad se considerará adecuada la publicación de estas a una página web.

Artículo 131-5. Causas de recusación de los miembros del Órgano de Supervisión

1. Los miembros del Órgano de Supervisión que participen en la inspección, la instrucción de expedientes o la intervención en cualquier procedimiento que pueda tener efectos en la entidad adherida al Código de Conducta podrán ser recusados por esta entidad o por un tercero con interés legítimo.

2. Serán causas de recusación haber participado, en algún momento de los tres años precedentes, como auditor en materia de protección de datos, redactor de un análisis de riesgo o de una evaluación de impacto o Delegado de Protección de Datos, o interlocutor principal en caso de actuar a través de una persona jurídica como tal, de la entidad objeto de control. Asimismo, se considerará en causa de recusación la persona física que haya participado como consultor en materia de protección de datos para la entidad objeto de control.

3. Sin perjuicio de lo dispuesto en el apartado anterior, serán causas de recusación cualquier causa que pueda suponer conflicto de intereses, así como falta de imparcialidad.

Artículo 131-6. Procedimiento de recusación de los miembros del Órgano de Supervisión

1. El procedimiento de recusación deberá iniciarse en el plazo máximo de cinco días hábiles desde la notificación del inicio del procedimiento o desde que la entidad tenga conocimiento de la participación del miembro del Órgano de Supervisión afectado debido a la recusación. Asimismo, se dispondrá de cinco días hábiles para solicitar la recusación del miembro del Órgano de Supervisión que se encuentre afectado por la causa de recusación desde el momento en que las condiciones de acuerdo con las que ésta se pide sean conocidas por la entidad o el tercero con interés legítimo en el procedimiento. La petición se formulará al Órgano de Supervisión por escrito, en formato digital o en papel, de manera que quede constancia del envío.

2. Los miembros del Órgano de Supervisión, a excepción del miembro o miembros sobre los que se dirija la recusación, decidirán sobre su procedencia. Las decisiones se emitirán por escrito y de manera motivada a las partes interesadas.

   El Órgano de Supervisión responderá de manera individualizada a cada miembro recusado, y participará el conjunto del Órgano en la decisión, excepto la persona sobre la que se decide la recusación. Los miembros del Órgano de Supervisión se abstendrán únicamente de participar en las votaciones en las que se decida sobre la procedencia de la recusación que los afecte directamente.

Artículo 131-7. Procedimiento de sustitución de los miembros recusados

Cuando, por razón de la recusación de los miembros del Órgano de Supervisión, este quede en situación en que menos de tres de sus miembros se encuentren habilitados para la instrucción o gestión de los expedientes, procedimientos, consultas o cualquier otra cuestión relacionada con el funcionamiento normal del órgano, habrá que sustituir tantos miembros como sean necesarios por otros que cumplan con las condiciones establecidas en el artículo 131-3 del presente Código de Conducta. Esta sustitución se

limitará a las actuaciones en que los miembros titulares del Órgano se encuentren recusados.

Las personas que actúen como sustitutas al Órgano de Supervisión tendrán la consideración de miembros de pleno derecho a todos los efectos, y se les aportará los recursos necesarios para que puedan desarrollar sus funciones con total independencia y autonomía de manera análoga a la de los miembros titulares del Órgano de Supervisión.

Capítulo II - Supervisión y control del cumplimiento del Código de Conducta

Artículo 132-1. Competencias del Órgano de Supervisión

1. El Órgano de supervisión es plenamente competente para determinar la adecuación de las entidades adheridas a las disposiciones del presente Código.

2. Para poder ejercer sus competencias de manera autónoma e independiente, el Órgano de Supervisión dispondrá de los recursos necesarios para el desarrollo de su actividad de control. Estos incluyen la gestión de recursos económicos, la disposición de tiempo necesario para la práctica de actuaciones inspectoras y el acceso a todo el resto de recursos que resulten necesarios para el correcto desarrollo de sus funciones.

3. El Órgano de Supervisión establecerá un plan anual o bienal que establezca las actuaciones que deben llevarse a cabo durante el periodo. En cualquier caso, deberá incorporar un programa de revisión de elementos concretos del Código de Conducta a las entidades adheridas. Con carácter general, las conclusiones formuladas a partir de las deficiencias detectadas en las entidades adheridas se emplearán para la elaboración de informes, recomendaciones y pautas de actuación para la mejora y solución de estas. Sin embargo, cuando las deficiencias detectadas en una entidad sean de carácter grave o respondan a una flagrante falta de diligencia de la entidad adherida, se iniciará contra esta un expediente instruyendo la deficiencia detectada, y se podrá imponer la sanción que corresponda.

4. Los planes anuales o bienales previstos en el apartado anterior podrán complementarse o sustituirse por planes de auditoría o inspección que tendrán por objeto la revisión del cumplimiento integral del Código de Conducta y abarcarán la más amplia representación posible de las entidades adheridas . Estos planes de auditoría o revisión deberán llevarse a cabo, como mínimo, de manera quinquenal.

5. El Órgano de supervisión es plenamente competente para iniciar procedimientos o expedientes de instrucción y sanción en caso de incumplimientos de las entidades adheridas. Estos procedimientos sancionadores podrán iniciarse siempre que se detecten incumplimientos que sean merecedores de sanción, independientemente de la vía por la que se haya tenido conocimiento.

6. A los efectos de atender peticiones o consultas por los interesados, personal o interlocutores de las entidades adheridas, el Órgano de Supervisión dispondrá de un canal de contacto habilitado.

7. El Órgano de Supervisión será competente para gestionar un canal de denuncias para dirigir información sobre cualquier incumplimiento en materia de protección de datos de las entidades adheridas. Este canal estará abierto al personal de la entidad adherida y a terceros, y deberá habilitar mecanismos que permitan la denuncia o alerta anónima. Asimismo, en la medida de lo posible, se habilitarán canales alternativos a los electrónicos, en especial los canales telefónico y presencial.

Artículo 132-2. Transparencia

1. El Órgano de supervisión hará pública toda actuación, ya sea respuesta a consultas, la instrucción de expedientes o cualquier otra actuación que tenga incidencia sobre la interpretación o aplicación del presente Código de Conducta.

2. Sin perjuicio de lo anterior, las publicaciones omitirán los datos que identifiquen tanto las personas físicas como jurídicas.

3. Los expedientes incoados por el Órgano de Supervisión requerirán la identificación de los miembros que participan, así como la identificación de la calidad en la que se participa, a los efectos de facilitar la información adecuada a las partes interesadas a efectos de lo dispuesto en los artículos 131-3 y 131-4 del presente Código de Conducta.

Capítulo III - Régimen sancionador

Artículo 133-1. Procedimiento sancionador

1. Las entidades adheridas al Código de Conducta estarán sujetas al presente régimen sancionador como consecuencia de las infracciones cometidas en relación con las disposiciones establecidas en el presente Código de Conducta en relación con la protección de datos personales en el marco de la prestación de servicios de asistencia o tratamiento de datos en el ámbito sanitario.

2. Corresponde al Órgano de Supervisión la imposición de sanciones en relación con conductas que puedan ser constitutivas de infracción conforme a lo establecido en este Código de Conducta.

3. El procedimiento sancionador se iniciará de oficio por el Órgano de Supervisión, en el que se requerirá a la entidad afectada que en el plazo de un mes desde el requerimiento, presente alegaciones por escrito respecto de los hechos expuestos en el procedimiento sancionador.

4. Sin perjuicio de lo indicado en el apartado anterior, el Órgano de Supervisión estará obligado a iniciar un procedimiento sancionador cuando reciba una denuncia, incluso anónima, por la que se comunique, de la manera en que se supere un juicio mínimo de credibilidad o cuando la denuncia formule una mínima actividad probatoria de cargo.

Artículo 133-2. Trámite de alegaciones

Una vez acordada la apertura del procedimiento sancionador por el Órgano de Supervisión, este notificará tal hecho a la entidad afectada y se le concederá un plazo de un mes, entendido como treinta días naturales, para que la entidad pueda presentar alegaciones o explicaciones complementarias por escrito entorno a los hechos que son objeto de investigación.

Si la entidad afectada responde a dicho requerimiento, el Órgano de Supervisión analizará y estudiará las alegaciones o explicaciones complementarias aportadas por la entidad requerida y, en el plazo de un mes desde el día siguiente a la recepción de las alegaciones, dará respuesta formal a la entidad afectada informando del resultado final del procedimiento sancionador. Esta comunicación formal indicará la infracción cometida y la sanción aparejada a dicha infracción, o bien la falta de responsabilidad de la entidad investigada y el cierre de las actuaciones. En cualquiera de las respuestas que se dé, el Órgano de Supervisión deberá motivar sus decisiones. En caso de que la entidad afectada no responda al requerimiento efectuado por el Órgano de Supervisión en el plazo de un mes desde el día siguiente a su notificación, el órgano sancionador deberá resolver el procedimiento sancionador, también, en el plazo de un mes a contar desde el día siguiente en que expiró el tiempo de respuesta brindado a la entidad investigada.

Artículo 133-3. Infracciones

Las infracciones tipificadas en este Código de Conducta se califican como leves, graves o muy graves.

1. Se consideran infracciones leves:

    a. No identificar las categorías de interesados de conformidad con lo dispuesto en el capítulo II del título I del libro segundo del presente Código de Conducta.
    b. Proceder al tratamiento de datos personales sin cumplir alguno de los requisitos de información a los interesados establecidos en el capítulo I del título II del libro segundo del presente Código de Conducta.
    c. No identificar adecuadamente a las personas transgénero o transexuales en los términos establecidos en el artículo 227-3 del libro segundo del presente Código de Conducta.
    d. Cualquier infracción que no constituya infracción grave o muy grave.

2. Se consideran infracciones graves:

a. Incumplir el deber de insolubilidad de los datos recogidos en el ámbito de la asistencia sanitaria privada con los datos recogidos en el marco de la prestación de servicios de salud de carácter público, y viceversa, en los términos previstos en el capítulo IV del título I del libro segundo del presente Código de Conducta.
b. No aplicar las medidas de garantía aplicables al tratamiento de datos de salud en los términos previstos en los capítulos I, II, III, V, VI, VII, VIII y IX del título II del libro segundo del presente Código de Conducta.
c. No aplicar una metodología adecuada en el análisis de riesgos y las evaluaciones de impacto, de conformidad con lo dispuesto en el capítulo VIII del título III del libro segundo del presente Código de Conducta ..
d. No permitir evaluar el grado de cumplimiento de este Código de Conducta al Órgano de Supervisión.
e. No responder en el plazo previsto cualquier requerimiento, explicando o presentando alegaciones por escrito en relación con los hechos expuestos en una reclamación.
f. No enmendar, sin causa justificada, una infracción leve que haya sido objeto de sanción en el plazo indicado por el Órgano de Supervisión.
g. Ser sancionado por la comisión de dos infracciones de carácter leve al presente Código de Conducta en un año.

3. Se consideran infracciones muy graves:

a. No aplicar las medidas de garantía de ejercicio de los derechos de autodeterminación informativa en los términos previstos en el capítulo IV del título II del libro segundo del presente Código de Conducta.
b. Incumplir de manera sistemática con las medidas de seguridad de acuerdo con los escenarios de riesgo descritos en este Código de Conducta.
c. No subsanar una infracción grave que haya sido objeto de sanción.
d. Ser sancionado por la comisión de dos infracciones de carácter grave al presente Código de Conducta en un año.

Artículo 133-4. Calificación de las sanciones

Las infracciones tipificadas en el artículo anterior tienen aparejadas las siguientes sanciones:

a. Sanción por infracción leve: amonestación y requerimiento a la entidad infractora para que subsane los hechos que dan lugar a la comisión de la infracción.
b. Sanción por infracción grave: suspensión temporal de la condición de entidad adherida al presente Código hasta que subsane los hechos que dan lugar a la comisión de la infracción.
c. Sanción por infracción muy grave: suspensión temporal de un año de la condición de entidad adherida al presente Código. En atención a la gravedad de la infracción, o la no reposición a una situación de cumplimiento, pueden conllevar la pérdida definitiva de la condición de entidad adherida al infractor.

Artículo 133-5. Competencia de las autoridades de control

El régimen sancionador establecido en el presente Código de Conducta se entiende sin perjuicio de los procedimientos y sanciones que las autoridades de control competentes puedan incoar en ejercicio de sus competencias, en especial respecto de las infracciones derivadas del incumplimiento de las disposiciones establecidas en la normativa vigente en materia de protección de datos personales.

Capítulo IV - Mecanismos de autocontrol

Artículo 134-1. Auditoría

1. Las entidades adheridas al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de la normativa de protección de datos.

2. El informe de auditoría incluirá las consideraciones oportunas respecto del grado de cumplimiento de la normativa en materia de protección de datos vigente, así como de lo establecido en el presente Código de Conducta de acuerdo con lo que resulte aplicable para la entidad adherida.

3. El Delegado de Protección de Datos de la entidad adherida participará en la auditoría y será responsable de elevar las conclusiones del informe al más alto nivel de dirección de la entidad. El Delegado de Protección de Datos será responsable de la custodia del informe, que deberá estar en todo momento a disposición del órgano de control del código de conducta en caso de que sea requerido.

Título IV - Régimen de actualización y modificación de este Código de Conducta

Capítulo I - Actualización del Código de Conducta

Artículo 141-1. Revisión del Código de Conducta

1. El presente Código será revisado, al menos, con periodicidad anual por el Órgano de Supervisión.

2. La revisión a la que se refiere el apartado anterior incluirá una valoración en relación con la vigencia del Código de Conducta respecto de las modificaciones legislativas que se hayan sucedido, a las interpretaciones doctrinales o jurisprudenciales relevantes en materia de protección de datos, a los cambios tecnológicos u organizativos relevantes en el sector y a los eventuales cambios sociales y contextuales que afecten al tratamiento de los datos personales.

   La revisión anual del presente Código de Conducta tendrá en cuenta las observaciones, comentarios, aportaciones y propuestas que las entidades adheridas

puedan hacer, incluyendo aquellas valoraciones referentes a la aplicación práctica del Código, su efectividad o la acogida del texto en el esfera interna de las entidades por los profesionales que lo integran.

Artículo 141-2. Modificación, ampliación o actualización del Código de Conducta

1. El presente código sólo podrá ser modificado o actualizado a iniciativa del Consorcio de Salud y de Atención Social de Cataluña. El Órgano de Supervisión instará al Consorcio de Salud y de Atención Social de Cataluña proceder a la modificación o actualización del Código de Conducta cuando se detecten carencias o cambios que hagan necesaria una adaptación de este Código.

2. Sin perjuicio de lo expuesto, las entidades adheridas pueden proponer modificaciones y actualizaciones del Código de Conducta. Se habilitará un canal para que las entidades adheridas puedan remitir una comunicación escrita al Órgano de Supervisión indicando razonadamente los motivos que fundamentan la propuesta de modificación o actualización. El Órgano de Supervisión dará respuesta motivada sobre la idoneidad de la propuesta en un plazo de tiempo razonable y, en ningún caso, en más de treinta días naturales. En caso de que la propuesta se considere idónea, se elevará al Consorcio de Salud y de Atención Social de Cataluña, y se instará a proceder a la modificación o actualización del Código de Conducta.

3. Toda modificación o actualización del Código de Conducta, en caso de ser aprobada por el Consorcio de Salud y de Atención Social de Cataluña, requerirá la pertinente comunicación a la autoridad de control competente para su aprobación definitiva.

4. De manera previa al traslado de la propuesta de modificación o actualización del Código de Conducta a la Autoridad Catalana de Protección de Datos, el Consorcio de Salud y de Atención Social de Cataluña trasladará la propuesta de modificación o actualización a las entidades adheridas, que dispondrán de quince días hábiles para hacer las aportaciones que consideren oportunas respecto del proyecto. El Consorcio de Salud y de Atención Social de Cataluña podrá incorporar, si lo considera adecuado, las modificaciones al proyecto que se deriven de las aportaciones recibidas.

5. Una vez aprobada la modificación o actualización del Código de Conducta por la Autoridad Catalana de Protección de Datos, el Consorcio de Salud y de Atención Social de Cataluña remitirá una copia del texto aprobado a las entidades adheridas. Las entidades adheridas dispondrán de un plazo de un mes desde la recepción de este texto para solicitar, si lo consideran adecuado, la baja como entidad adherida.

Título V - Derechos y deberes de las entidades adheridas al Código de Conducta

Capítulo I - Derechos de las entidades adheridas al Código de Conducta

Artículo 151-1. Derechos de las entidades adheridas

Toda entidad adherida al Código de Conducta que se encuentre en cumplimiento de las obligaciones de adhesión al Código de Conducta tendrá los siguientes derechos:

a) Derecho a participar en las actividades que se organicen relacionadas con el desarrollo y la aplicación del Código de Conducta.
b) Derecho a ser informado sobre la composición del Órgano de Supervisión, de su estado de cuentas y del desarrollo de su actividad.
c) Derecho a ser oído con carácter previo a la adopción de medidas disciplinarias contra la entidad y a ser informado de los hechos que den lugar a la imposición de estas medidas, y deberá ser motivado el acuerdo que, en su caso, imponga la sanción.
d) Derecho a impugnar los acuerdos que adopte el Órgano de Supervisión y que la entidad estime contrarios a la Ley o al mismo Código de Conducta.

Capítulo II - Deberes de las entidades adheridas al Código de Conducta

Artículo 152-1. Deberes de las entidades adheridas

Son deberes de las entidades adheridas:

a) Compartir las finalidades del Código de Conducta y colaborar para la consecución de sus objetivos.
b) Satisfacer la cuota de inscripción y las cuotas de adheridos que se establezcan y el resto de aportaciones para el mantenimiento del Código de Conducta y sus órganos.
c) Cumplir el resto de obligaciones que resulten de las disposiciones normativas.
d) Acatar y cumplir los acuerdos válidamente adoptados por el Órgano de Supervisión.

Anexo 1. Formulario de solicitud de adhesión al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña

Sr./Sra ....., en nombre y representación de ....., con CIF ..... i con domicilio en .....

MANIFIESTA

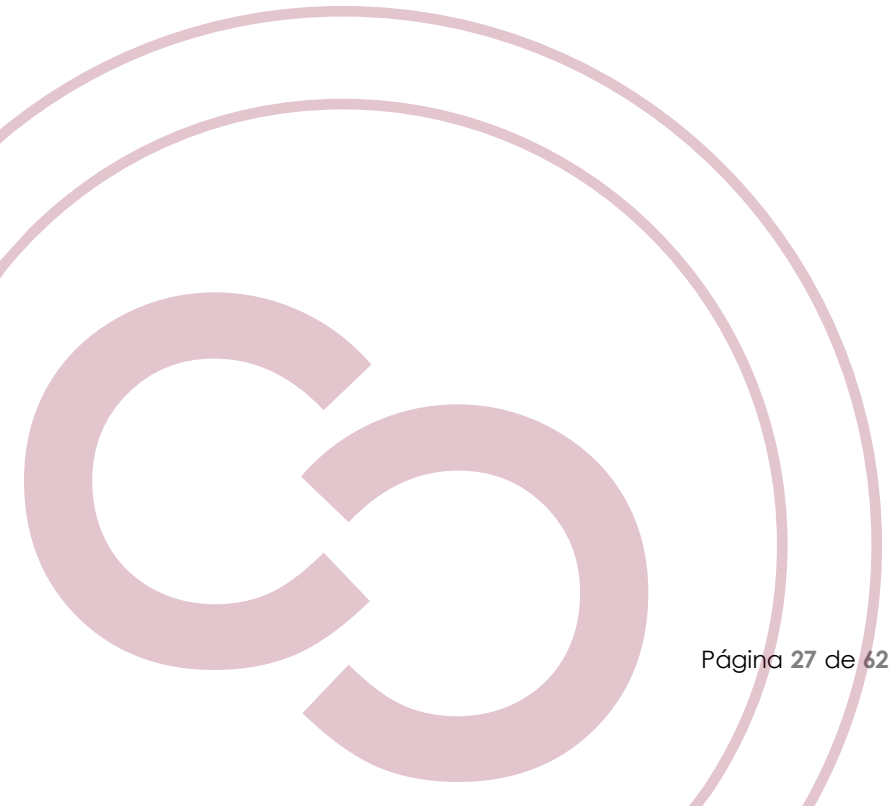
1. Que cumple con todos los requisitos establecidos para el ejercicio de la actividad de prestación de servicios del ámbito de salud.
2. Que cumple con las disposiciones establecidas en el Código de Conducta, y que acepta y se somete a todo lo dispuesto en materia de protección de datos personales.
3. Que desea adherirse al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña.

SOLICITA AL ÓRGANO DE SUPERVISIÓN

Que se tenga por presentada esta solicitud de adhesión al Código de Conducta del Consorcio de Salud y de Atención Social de Cataluña y se proceda a estimar la adhesión.

En ....., a ..... de ..... de.....

Firma



Anexo 2. Formulario de solicitud de baja como entidad adherida al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña

Sr./Sra ....., en nombre y representación de ....., con CIF ..... i con domicilio en .....

MANIFIESTA

1. Que es voluntad de la entidad representada desvincularse del Código de Conducta del Consorcio de Salud y de Atención Social de Cataluña.
2. Que la baja como entidad adherida será efectiva al final del presente año natural[1].
3. Que, en el momento de hacerse efectiva la baja, la entidad ya no dispondrá de indicadores o menciones que la identifiquen como entidad adherida al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña.

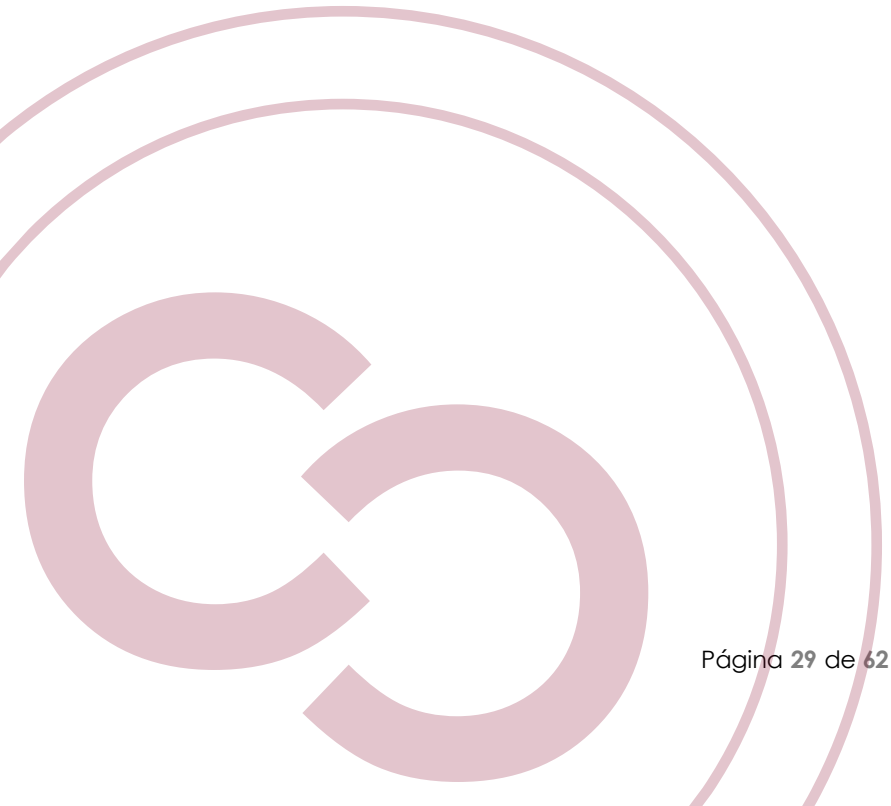
SOLICITA AL ÓRGANO DE SUPERVISIÓN

Que se tenga por presentada esta solicitud de baja como entidad adherida al Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña y se proceda a efectos de dar cumplimiento a lo que se solicita.

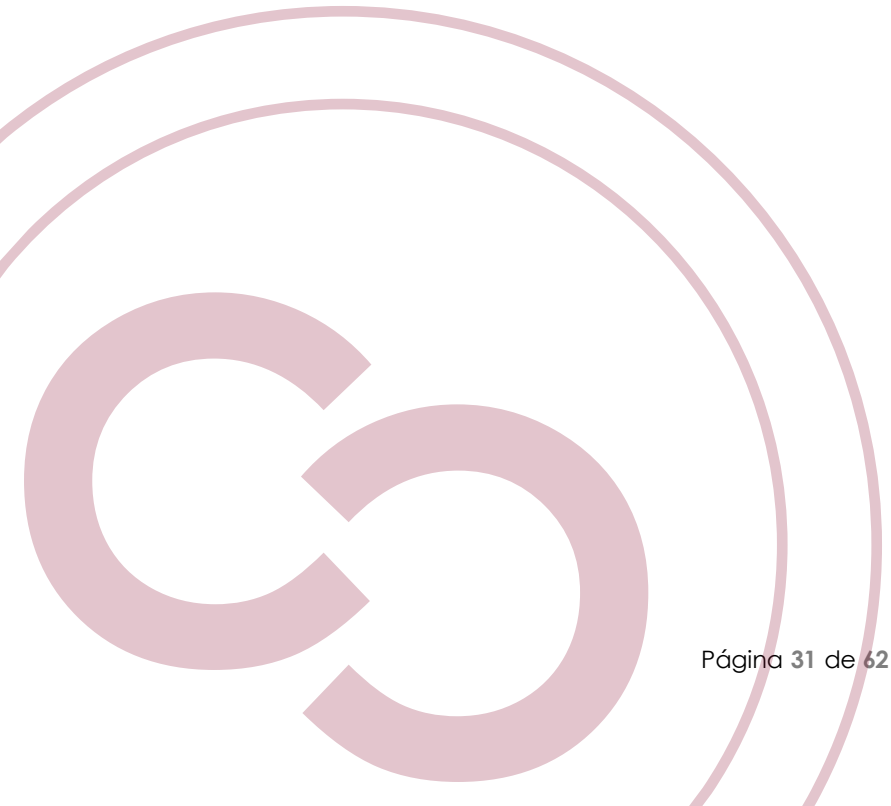
En ....., a ..... de ..... de.....

Firma

[1] Siempre que la solicitud se entregue con anterioridad con fecha de 30 de noviembre.



Libro segundo



Índice

Libro segundo. Condiciones aplicables al tratamiento de datos
Título I - Especificidades del tratamiento de datos relativos a la salud

Capítulo I - Datos de salud

Artículo 211-1. Datos de salud

1. A los efectos del presente Código de Conducta se considerará dato de salud toda información o conjunto de informaciones que permitan conocer o determinar, sin esfuerzos desproporcionados, el estado completo o parcial de bienestar físico, mental y social, así como la ausencia, o no, de afecciones o enfermedades.

2. Sin perjuicio de su consideración de acuerdo con las categorías de datos previstas en la normativa vigente, deberán aplicarse las previsiones en materia de tratamiento de datos previstas en el presente Código de Conducta a las categorías de datos siguientes:

    a. todos aquellos datos que, con referencia a una persona física identificada o identificable, indiquen el grado de adaptación de la persona al medio biológico, en el estado fisiológico de equilibrio y a la alimentación, cuando resulte relevante para el tratamiento, diagnóstico o prestación de servicios de carácter asistencial o en el marco de la búsqueda o investigación en salud;

    b. los datos relativos a los hábitos de la persona que tengan un impacto en el estado de salud de la persona o afecten o puedan afectar los datos señalados en el apartado anterior, cuando resulte relevante para el tratamiento, diagnóstico o prestación de servicios de carácter asistencial o en el marco de la búsqueda o investigación en salud, y

    c. los datos ambientales, poblacionales, geográficos, étnicos, de carácter religioso o filosófico o de cualquier otro tipo que tenga una incidencia específica y concreta sobre el estado de salud de una persona o resulte relevante para el tratamiento, diagnóstico o prestación de servicios de carácter asistencial o en el marco de la búsqueda o investigación en salud.

3. Cuando un conjunto de datos permita establecer, relacionar, prever, determinar, entre otros, el estado de salud de una persona, habrá que aplicar a estos datos las medidas de seguridad previstas en este Código de Conducta, incluso cuando, de forma separada o independiente, no permitan la identificación de la persona.

4. El tratamiento de datos a los que se refiere este artículo quedará sujeto a lo previsto en este Libro.

Capítulo II - Interesados sujetos al tratamiento de datos

Artículo 212-1. Categorías de interesados

1. Todo tratamiento de datos realizado en el marco de la prestación de servicios asistenciales, de diagnóstico o de salud deberá tener en cuenta los efectos que tenga respecto de los derechos, libertades e intereses legítimos de las categorías de interesados afectadas por cada tratamiento, teniendo en cuenta las características que previsiblemente tendrán estas personas en función de la tipología del servicio prestado en el marco del tratamiento de los datos personales.

2. Las categorías de interesados a las que se refiere el apartado anterior incluyen los pacientes y las personas vinculadas a estos, así como aquellas otras categorías de interesados que puedan verse afectadas por el tratamiento de datos.

3. A los efectos de aplicar las medidas de seguridad específicas del presente Código de Conducta resultará necesario que el responsable o encargado del tratamiento identifique correctamente las categorías de interesados en las que, de manera esperable y general, afecten a los tratamientos de datos previstos.

Capítulo III - Circunstancias específicas a tener en cuenta respecto de las categorías de interesados de pacientes y personas vinculadas

Artículo 213-1. Menores de edad

Se entenderá persona menor de edad en el ámbito de la protección de datos la persona con una edad inferior a los catorce años. Sin embargo, habrá que tener en consideración el tramo de los doce a los catorce años como una edad en que, de acuerdo con el grado de madurez que presente la persona, debe ser informada del alcance del tratamiento de sus datos, sin perjuicio que corresponda a los progenitores o tutores legales ejercer los derechos de autodeterminación informativa y el otorgamiento del consentimiento, cuando proceda, para el tratamiento de los datos personales.

Artículo 213-2. Personas frágiles

1. Se entenderá persona frágil a los efectos del presente Código de Conducta toda persona que tenga o pueda tener afectadas sus condiciones cognitivas o volitivas por razón de situación personal o familiar, económica, enfermedad, estado físico o psíquico, adicción o cualquier otra situación de dependencia o afectación.

2. Tendrán consideración de personas frágiles todas aquellas personas que por motivos socioeconómicos, culturales, lingüísticos, educativos o de cualquier otro tipo puedan tener dificultad para comprender el alcance del tratamiento de datos

o para comprender la información relativa a este tratamiento o la posibilidad de ejercer derechos reconocidos por la legislación vigente.

3. Tendrán consideración de personas frágiles todas aquellas personas que se encuentren en situación de brecha digital o de género o de cualquier otro tipo, cuando esta situación suponga o pueda suponer una afectación en relación con el tratamiento de datos proyectado por el responsable del tratamiento.

Artículo 213-3. Trabajadores

1. A los efectos del presente Código de Conducta tendrán la consideración de trabajadores las personas que presten servicio al responsable del tratamiento o a una entidad que participe en el régimen laboral o régimen especial de trabajador autónomo económicamente dependiente, así como las personas que presten servicios al responsable del tratamiento o encargado del tratamiento.

2. La consideración de paciente persona trabajadora se tendrá en cuenta tanto en la relación asistencial derivada del cumplimiento de las obligaciones de salud laboral o prevención de riesgos laborales como de la derivada de la prestación asistencial o de servicios de salud de carácter ordinario.

Artículo 213-4. Personas con riesgo de estigmatización

Se considerarán personas en riesgo de estigmatización, a los efectos de aplicación del presente Código de Conducta, aquellas que:

a. sufran enfermedades mentales o que tengan afectaciones de carácter psíquico o psicológico, cuando esta condición no sea obstáculo para el seguimiento de una vida normal;

b. estén diagnosticadas, o existan sospechas, de sufrir de sida, VIH, hepatitis, sufran enfermedades crónicas o infecciosas tradicionalmente vinculadas a estilos de vida o a la orientación sexual, con independencia de que esta vinculación responda o no a la realidad de la enfermedad;

c. estén diagnosticadas de condiciones genéticas que prevean, determinen o identifiquen posibles condiciones médicas futuras que puedan afectar a los derechos, libertades e intereses legítimos de las personas, y

d. estén afectadas por condiciones médicas derivadas de las condiciones económicas, sociales, culturales o derivadas del entorno socioeconómico de la persona.

Artículo 213-5. Víctimas de delitos

Se considerarán personas víctimas de delitos, a los efectos de aplicación del presente Código de Conducta, aquellas que reciban asistencia sanitaria, urgente o no, por razón de haber sufrido un delito o posible delito, o derivado de actos de violencia.

Artículo 213-6. Víctimas de violencia de género

Se considerarán personas víctimas de delitos, a los efectos de aplicación del presente Código de Conducta, aquellas que reciban asistencia sanitaria, urgente o no, por razón de haber sufrido delito o posible delito de violencia de género, o derivado de actos de violencia producidos en el ámbito del hogar o la pareja, cuando la víctima sea una mujer.

Artículo 213-7. Personas públicas

Se considerará persona pública, a los efectos del presente Código de Conducta, cualquier persona que tenga relevancia social o tenga un reconocimiento público o ocupe un espacio en el debate público, incluso en el ámbito territorial o local, ocupe un cargo o profesión de relevancia pública o reciba asistencia sanitaria fruto de un evento o suceso de interés periodístico o público.

Capítulo IV - Prestaciones asistenciales de carácter privado

Artículo 214-1. Insolubilidad de los datos procedentes de tratamientos de carácter privado respecto de los datos tratados en ejercicio de misión de interés público

1. La prestación de servicios de salud de carácter privado debe suponer el tratamiento diferenciado de estos datos respecto de aquellos datos tratados en las líneas de carácter público, por lo que los datos personales tratados o recaudadas en un servicio de naturaleza privada no se encuentren disponibles en la prestación de servicios asistenciales carácter público, y viceversa, salvo que el interesado así lo haya consentido o sea aplicable otra base jurídica que lo permita.

2. Las previsiones del apartado anterior serán de aplicación tanto en los casos en que un mismo responsable del tratamiento lleve a cabo actos asistenciales de carácter privado y público como en el caso de que estos actos asistenciales sean llevados a cabo por responsables del tratamiento diferentes.

3. En la medida en que lo permitan la tecnología empleada, los sistemas de tratamiento de la información y la tipología de los datos tratados, es necesario habilitar un sistema que permita trasladar los datos a la Plataforma Digital de Salud del Departamento de Salud de la Generalidad de Cataluña y con las plataformas análogas que puedan establecerse en el Sistema Nacional de Salud, cuando así lo solicite el interesado.

Título II - Medidas de garantía aplicables al tratamiento de datos de salud

Capítulo I - Medidas para garantizar un tratamiento de datos leal y transparente

Artículo 221-1. Información a los mostradores

1. A todos los puntos de recogida de datos directamente de los interesados, así como a los mostradores de atención al usuario o de recepción, se instalarán carteles informativos con, como mínimo, la información básica relativa al tratamiento de datos de salud y los tratamientos accesorios, incluyendo la identificación del responsable del tratamiento, las finalidades previstas y la potestad de los interesados de ejercer los derechos que les asisten, en los términos establecidos en el artículo 11 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. En caso de facilitarse la información básica, se incluirá la referencia a la información adicional y la manera de acceder a ella.

2. Los carteles informativos se mantendrán actualizados y tendrán unas dimensiones y tipologías de letra y ubicación adecuadas para garantizar la correcta visualización y lectura de los interesados.

3. La información deberá presentarse en un formato que permita que las personas puedan alcanzar el conocimiento de manera autónoma. Cuando los destinatarios tengan de manera habitual o previsible problemas de visión, se deberá presentar la información en formato Braille o en un formato que permita que puedan acceder a ella por sí solas.

4. En la medida de lo posible, y en proporción a las necesidades que se deriven del ámbito geográfico, social, cultural y económico, habrá que facilitar la información en los idiomas adecuados para garantizar que los interesados puedan acceder de manera efectiva a la información facilitada.

5. La utilización de carteles informativos para facilitar la información sobre el tratamiento de los datos a los pacientes y usuarios de acuerdo con los apartados anteriores supondrá la aplicación de un mecanismo adicional de transparencia que en ningún caso deberá ser entendido como un canal principal o prioritario para cumplir con las disposiciones de los artículos 13 y 14 del Reglamento general de protección de datos cuando existan otros mecanismos que, previsiblemente, sean más adecuados para facilitar la información a los interesados, en especial teniendo en cuenta la naturaleza de los datos tratados y las finalidades de cada tratamiento.

Artículo 221-2. Disponibilidad de la información adicional

1. Sin perjuicio de la existencia de carteles informativos, cuando sea apropiado, u otros soportes donde conste la información sobre el tratamiento de datos, cuando dicha información se presente en la modalidad básica prevista en el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, será necesario facilitar el acceso de los interesados a la información adicional a través de mecanismos sencillos, como un aviso en la página web o mediante hojas a disposición de los

interesados. La información facilitada a los interesados deberá presentarse de manera clara y comprensible, se expresará en lenguaje natural y con una complejidad semántica y gramatical adecuada a las capacidades de comprensión que, previsiblemente, presenten las categorías de interesados a las que va dirigida .

2. En la medida de lo posible, se instalarán carteles con la información completa del tratamiento de datos con fines asistenciales a los espacios comunes como salas de espera o pasillos, por lo que la información adicional esté disponible sin necesidad de acceder a ella por medios digitales, con el fin de facilitar el acceso a esta información a las personas frágiles o con dificultad para el acceso a internet.

3. En relación con el apartado anterior, cuando los interesados a los que se dirige la información, por razón del servicio prestado, ámbito geográfico o cualquier otra circunstancia, presenten de manera habitual situaciones de brecha digital que les impida acceder a la información adicional de manera sencilla a través de servicios en línea, se deberá informar de manera clara que los interesados pueden disponer de manera gratuita de copias en papel de la información adicional sobre el tratamiento de datos.

4. Cuando la información adicional sea accesible por canales digitales será necesario identificar la vía de acceso de forma que resulte de fácil acceso y recordatorio. En este sentido, cuando la información sea accesible a través de un localizador uniforme de recursos (URL), éste deberá presentarse de la manera más cercana posible al lenguaje natural, de forma breve y de una complejidad adecuada a la categoría de interesados a la que va destinada y que permita ser recordada con facilidad.

5. Cuando, en cumplimiento de los preceptos anteriores, se facilite la información adicional en formato papel y cuando los destinatarios tengan de manera habitual o previsible problemas de visión, se deberá presentar la información en formato Braille o en un formato que permita que puedan acceder a ella por si solas.

6. En la medida de lo posible, y en proporción a las necesidades que se deriven del ámbito geográfico, social, cultural y económico, habrá que facilitar la información en los idiomas adecuados para garantizar que los interesados puedan acceder de manera efectiva a la información facilitada. Se considerará cumplido este precepto cuando la información se facilite por internet de forma que pueda ser traducida por servicios de traducción en línea de manera que los resultados se presenten, generalmente, de forma que sea posible comprender el sentido del texto de manera suficiente.

Artículo 221-3. Información a menores

1. Cuando el tratamiento de los datos de salud se dirija de manera sustancial o habitual a categorías de interesados de menores de edad será necesario adecuar la información facilitada a efectos de hacerla tan comprensible como

sea posible de acuerdo con la edad y grado de entendimiento que previsiblemente tengan los interesados.

2. A los efectos de dar cumplimiento a las previsiones del apartado anterior será necesario adecuar el lenguaje para hacerlo comprensible para las personas menores y, en la medida de lo posible, se deberá incluir imágenes o pictogramas que faciliten la comprensión de la información facilitada .

Artículo 221-4. Información a trabajadores

1. Cuando el tratamiento de datos de salud afecte trabajadores en el marco de las medidas relativas a la vigilancia de la salud, se deberá indicar de manera clara, en su caso, qué tratamientos se basan en el consentimiento y cuáles son las consecuencias de no otorgarlo.

2. En caso de que sólo una parte o finalidad concreta de las diversas que configuran el tratamiento se base en el consentimiento en los términos establecidos en el apartado anterior, será necesario identificar qué tratamiento o finalidad se encuentra sujeto a este consentimiento por lo que no se lleve a error respecto del alcance del consentimiento otorgado.

3. A efectos de lo dispuesto en los artículos anteriores, se recogerá el consentimiento del trabajador para la revisión periódica de vigilancia de la salud en el momento de solicitarle si quiere someterse a la revisión médica.

4. Cuando, por razón de la legislación vigente y, en especial por la relevancia en el ámbito sanitario, en el marco de la vigilancia de la salud de los trabajadores expuestos a agentes biológicos, agentes cancerígenos y radiaciones ionizantes, el desarrollo del control médico en el marco de la salud laboral sea de carácter obligatorio, el trabajador debe ser informado del carácter obligatorio de este control médico.

Artículo 221-5. Información a personas frágiles

1. Cuando el tratamiento de los datos de salud se dirija de manera sustancial o habitual a categorías de interesados constituidas por personas frágiles habrá que adecuar la información facilitada a efectos de hacerla tan comprensible como sea posible de acuerdo con la situación personal, formación, capacidad y grado de entendimiento que previsiblemente tengan los interesados. Esta adecuación deberá abarcar tanto la forma en que se exprese el contenido de la información facilitada como el soporte en el que se presenta, que debe ser adecuado a las capacidades y posibilidades de la categoría de persona interesada a la que va dirigida.

2. Cuando sea posible se harán partícipes de la información sobre el tratamiento de los datos las personas vinculadas al interesado que se ocupen de su cuidado y atención.

3. Cuando la persona se encuentre en una situación de fragilidad temporal que previsiblemente será revertida será necesario establecer mecanismos que permitan asegurar que accede a la información relativa a los tratamientos de datos, como la inclusión de carteles informativos en los espacios de atención de carácter urgente y en las habitaciones, indicando en cualquier caso la forma en la que sea accesible la información completa sobre el tratamiento de los datos personales.

4. Cuando los servicios de salud ofrecidos tengan como destinatarias, de manera habitual o sustancial, personas con dificultades sensoriales, en especial ceguera o sordera, la información se facilitará de forma que pueda ser comprendida de manera autónoma por el interesado, tanto respecto de la forma en que se exprese esta información como respecto del soporte en el que se presenta.

Capítulo II - Medidas para garantizar un tratamiento de datos lícito

Artículo 222-1. Obtención del consentimiento

1. El consentimiento del interesado supone una base de licitud del tratamiento de datos que, en el marco de la prestación de servicios en el ámbito de la salud tiene un carácter residual, con poca incidencia en relación con los tratamientos de datos necesarios para la correcta asistencia sanitaria de los interesados. El tratamiento de datos asistencial encontrará, normalmente, cobertura en la misión de interés público y el interés vital del interesado, así como la ejecución de un contrato en el marco de la prestación de servicios de salud de carácter privado.

2. Sin perjuicio de lo expuesto, cuando la obtención del consentimiento de la persona interesada implique la base de licitud para el tratamiento de sus datos personales, el responsable del tratamiento deberá asegurar que el consentimiento se presta una vez la persona interesada ha recibido la información oportuna relativa al tratamiento, de conformidad con el artículo 12 del Reglamento general de protección de datos. Este consentimiento deberá recogerse de manera que se pueda acreditar en cualquier momento su validez, prestando especial atención en las características que previsiblemente presenten los interesados en función del servicio o servicios de carácter asistencial a los que accedan, adaptando el soporte en que se recoja el consentimiento a estas características.

3. Lo dispuesto en el apartado anterior se entiende sin perjuicio del consentimiento informado que exige la normativa sanitaria para la prestación de determinados actos asistenciales, consentimiento que implica un supuesto diferente al regulado en el presente artículo.

Artículo 222-2. Consentimiento otorgado por los pacientes o usuarios de los servicios

1. Cuando se obtenga el consentimiento para el tratamiento de datos con diversas finalidades, se facilitarán mecanismos que permitan la manifestación del

consentimiento de forma separada e independiente respecto de cada finalidad perseguida con el tratamiento de los datos, de manera que permitan al interesado conocer fácilmente el alcance de cada ámbito de consentimiento prestado vinculado a una finalidad diferente.

2. Cuando en el marco de la asistencia se pida el consentimiento para otros fines o tratamientos, el consentimiento sólo se podrá considerar válido cuando la información facilitada haga una referencia explícita a que el consentimiento para el tratamiento de los datos no es necesario, o no es condición necesaria, para la prestación de los servicios de carácter asistencial, ni supondrá una reducción en la calidad de estos servicios.

Artículo 222-3. Consentimiento otorgado por personas frágiles

1. Cuando el tratamiento de los datos de salud se dirija de manera sustancial o habitual a categorías de interesados constituidas por personas frágiles habrá que adecuar la forma de obtener el consentimiento de manera que pueda acreditarse que éste se corresponde con la verdadera voluntad del interesado en relación con la situación personal, formación, capacidad y grado de entendimiento que previsiblemente tengan los interesados.

2. Cuando existan dudas razonables sobre la capacidad de prestar el consentimiento del interesado se consultará al acompañante o persona vinculada al interesado para que manifieste las consideraciones oportunas sobre la validez del consentimiento. Si después de esta consulta se mantienen las dudas sobre la capacidad del paciente para otorgar el consentimiento, el tratamiento no se basará en el consentimiento, sino en otra base de licitud, como, en su caso, el interés vital del interesado u otra persona física.

3. El consentimiento de las personas con dificultades sensoriales sólo se reputará válido cuando se pueda acreditar que han podido acceder a la información adecuada sobre el tratamiento y sobre el alcance del consentimiento.

Artículo 222-4. Menores

Cuando los interesados tengan menos de catorce años en los tratamiento de datos basados en el consentimiento, se hará partícipes a los menores sobre la decisión en la medida en que lo permita su condición de madurez y de acuerdo con los requerimientos de los titulares de la patria potestad o tutela.

Artículo 222-5. Consentimiento obtenido de trabajadores

El consentimiento obtenido de los trabajadores de la entidad sólo será válido cuando, además de la información legalmente establecida, se informe a los trabajadores que la negativa al consentimiento no tendrá ningún efecto negativo respecto de la relación laboral.

Artículo 222-6. Retirada del consentimiento

La retirada del consentimiento por el interesado se hará con las mismas condiciones que las previstas para la obtención del consentimiento y en un formato o mecanismo que permita al interesado acreditar la retirada de su consentimiento y el momento temporal en el que el consentimiento otorgado deja de ser vigente.

Artículo 222-7. Tratamiento de datos de acuerdo con el interés vital del interesado u otra persona física

Cuando el tratamiento de los datos personales se base en el interés vital del interesado o de otra persona física será necesario basar el tratamiento de los datos del interesado en otra base de licitud una vez el interesado recupere la capacidad de otorgar el consentimiento.

Artículo 222-8. Efectos del Código de Conducta sobre las transferencias internacionales de datos

El presente Código de Conducta no constituye, en relación con lo dispuesto en el artículo 46.2.e del Reglamento general de protección de datos, un mecanismo que garantice la aplicación de garantías adecuadas para las transferencias internacionales de datos. Toda transferencia internacional de datos que haga el responsable del tratamiento a un tercer país u organización internacional deberá basarse en lo dispuesto en los artículos 44 y siguientes del Reglamento general de protección de datos.

Capítulo III - Medidas para garantizar la minimización de datos

Artículo 223-1. Comunicaciones de datos necesarios para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

En las comunicaciones de datos derivados de obligaciones legales, se deberá informar de la manera más clara y específica posible sobre estas a las personas interesadas, así como velar por que en la comunicación de datos se entreguen los datos estrictamente necesarios para el logro de la finalidad para la que son solicitados.

Artículo 223-2. Formularios de campo libre

1. Se limitará el uso de formularios de campo libre en las vías de contacto de los interesados con el responsable o encargado del tratamiento a fin de limitar en la medida de lo posible la difusión de datos personales por el propio interesado, su representante o la persona vinculada.

2. El uso de formularios de campo libre se podrá habilitar previa ponderación y evaluación del cumplimiento con el principio de minimización de datos.

Capítulo IV - Medidas para garantizar el cumplimiento de los derechos de autodeterminación informativa

Artículo 224-1. Mecanismos de ejercicio de los derechos de autodeterminación informativa

1. Con carácter general, el ejercicio de derechos de autodeterminación informativa para los interesados se hará conforme a lo establecido en los artículos 15 a 22 del Reglamento general de protección de datos, así como los artículos 12 a 18 de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

2. Los centros sanitarios deberán disponer de protocolos o procedimientos documentados que establezcan los mecanismos adecuados de gestión de los derechos de autodeterminación informativa de manera que se cumplan los requisitos formales y de fondo de respuesta a los interesados, así como los plazos establecidos en la norma y, en su caso, la información adecuada respecto de la prórroga de los mismos.
3. Los centros pondrán a disposición de los interesados formularios para el ejercicio de los derechos de autodeterminación informativa, sin perjuicio de tener que dar trámite, en igualdad de condiciones, a las peticiones formuladas por los interesados a través de formularios, escritos o cualquier otro formato y medio diferente del facilitado por la entidad, cuando el interesado aporte toda la información necesaria para la correcta tramitación del derecho.

Artículo 224-2. Acceso a la historia clínica

Los derechos de acceso a la totalidad o parte de la historia clínica dispondrán de mecanismos específicos que faciliten el ejercicio de los interesados.

Artículo 224-3. Derecho de rectificación sobre información médica

1. Es necesario disponer de un mecanismo específico, sencillo y ágil que permita a los interesados solicitar la corrección de los datos incorrectos de carácter administrativo, como los datos de contacto, teléfono y otras similares.

2. Será necesario disponer, también, de un mecanismo específico que permita a los interesados solicitar la subsanación de los datos incorrectos que se refieran al estado de salud, diagnóstico, tratamiento u otra característica o situación análoga del interesado. En la decisión de proceder a la corrección de los datos o en la denegación de la petición prevalecerá, en todo caso, el criterio médico.

Artículo 224-4. Derecho de supresión sobre información médica

Ante las peticiones de ejercicio de derechos de supresión que abarquen la totalidad o parte de los datos incorporados en la historia clínica se tendrá en consideración el criterio médico en la decisión sobre la procedencia de la supresión o la denegación de la petición.

Artículo 224-5. Derecho de oposición sobre información médica

Ante las peticiones de ejercicio de derechos de oposición al tratamiento de los datos que abarquen la totalidad o parte de la información incorporada en la historia clínica se tendrá en consideración el criterio médico en la decisión sobre la procedencia de la oposición o la denegación de la petición.

Capítulo V - Marco común de referencia para el tratamiento de los datos

Artículo 225-1. Marco de referencia respecto de la seguridad de los datos

1. El tratamiento de datos de salud en el marco de la prestación de servicios asistenciales, por las entidades adheridas al presente Código de Conducta e independientemente de la consideración de sector público, se hará de acuerdo con las medidas de seguridad previstas en el Esquema Nacional de Seguridad, aplicadas en la categoría que corresponda de acuerdo con los criterios de determinación del riesgo que resulten aplicables.

2. En los casos en que un tercero preste servicios a una entidad adherida que impliquen acceso a datos personales a raíz de una relación contractual, este tercero deberá aplicar medidas de seguridad que se ajusten al nivel de seguridad de las aplicadas por la entidad adherida en los términos previstos en la disposición adicional 1ª de la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Por tanto, las medidas de seguridad que debe adoptar el tercero que trate datos por cuenta de una entidad adherida deberán ajustarse a las previstas en el Esquema Nacional de Seguridad.

Artículo 225-2. Formación de los trabajadores y personal

1. Los trabajadores y personal del responsable o encargado del tratamiento de datos personales recibirá una formación general sobre las medidas expuestas en los capítulos anteriores de manera periódica. Esta periodicidad no podrá superar los dos años.

2. Será necesario impartir a los trabajadores y personal del responsable o encargado del tratamiento de datos personales una formación general sobre las medidas expuestas en los capítulos anteriores cuando la aplicación en la organización se modifique de manera sustancial o cuando otros elementos organizativos, materiales o de cualquier otro tipo lo hagan necesario.

Capítulo VI - Medidas para garantizar la confidencialidad e integridad de los datos

Artículo 226-1. Seudonimización y anonimización

1. En la medida de lo posible se aplicarán medidas de seudonimización de los datos personales, de forma que se impida la identificación, por personas no autorizadas, de las personas interesadas, en especial cuando los datos se sitúen

en espacios que permitan el acceso a terceros, como los carros de medicación o las bandejas de comida, entre otros.

La anonimización de datos médicos se hará de manera en que no aparezcan datos relativos a nombres, espacios geográficos, fechas, números de teléfono y fax, direcciones de correo electrónico, números de la Seguridad Social, números de registros médicos o de historia clínica , números de póliza de seguros, números de cuenta, identificadores de certificados o licencias, identificadores de vehículos o placas de matrícula, identificadores de dispositivo o número de serie, direcciones web y URL, direcciones de protocolo de internet, identificadores biométricos, fotografías de cara completa o imágenes comparables y cualquier otro código o identificador único o característica única, así como cualquier otro dato que, por sí sola o en combinación con otras, permita reidentificar la persona afectada.

Artículo 226-2. Acceso de las personas vinculadas

1. El acceso a la información de salud de los pacientes por las personas vinculadas se hará de manera que se respete la voluntad del paciente, informando sobre la posibilidad de que se facilite información a las personas vinculadas y sobre la manera en que el paciente puede oponerse a este hecho.

   La información a las personas vinculadas requerirá que la entidad elabore un protocolo, una instrucción técnica, un manual de buenas prácticas o un instrumento análogo que la regule, que deberá ser conocido por el personal que la deba aplicar.

2. La facilitación de la información relativa a la habitación o ubicación de un paciente dado o ingresado en las dependencias de la entidad se regulará por un protocolo, una instrucción técnica, un manual de buenas prácticas o un instrumento análogo que específicamente regule esta comunicación de datos, que deberá ser conocido por el personal que lo deba aplicar.

3. A fin de facilitar a las personas vinculadas el acceso a las informaciones establecidas en el presente artículo, hay que facilitar información de manera clara sobre la documentación o los requisitos necesarios para acceder a la información. Estos mismos soportes incorporarán la información adecuada sobre el tratamiento de los datos identificativos de la persona vinculada.

Artículo 226-3. Encriptación de los datos

Cuando se facilite el acceso a información que contenga datos de salud de los interesados a través de medios electrónicos, la información deberá estar encriptada. A los efectos de encriptar la información será preferible el uso de tecnologías TLS (Transport Layer Security) y, en la medida de lo posible, la inclusión de mecanismos de autenticación por certificado digital tanto de los servidores receptores como los emisores.

Artículo 226-4. Emisión de justificantes a petición de la persona atendida

1. Los justificantes de visita emitidos por petición del propio paciente podrán incluir la identificación y dirección del centro de salud en el que se le ha asistido, la fecha y hora de la asistencia y nombre y apellidos de la persona atendida. Adicionalmente, a petición del paciente, se podrá ampliar esta información.

2. En relación con lo indicado en el apartado anterior, y atendiendo al principio de minimización de datos, se permitirá incluir en los justificantes médicos información sobre

    a. el servicio o especialidad en el que ha sido atendido el paciente;

    b. el diagnóstico derivado de la asistencia, y

    c. la fecha de ingreso del paciente, así como, en su caso, la fecha de alta.

3. Será altamente recomendable que las entidades establezcan protocolos para concretar, regular y estandarizar el contenido de los justificantes descritos en los apartados anteriores de manera que el personal siga unas instrucciones unánimes en el momento de elaborar estos justificantes.

Artículo 226-5. Emisión de justificantes a petición de las personas vinculadas al paciente

1. Los justificantes de visita emitidos por petición de la persona vinculada incluirán, atendiendo siempre el principio de minimización de datos y teniendo en cuenta la finalidad para la que se solicita el justificante, la identificación y dirección del centro de salud en el que se le ha asistido, la fecha y hora de la asistencia y nombre y apellidos de la persona atendida.

2. Cuando por razón de la identificación del centro emisor o la especialización del prestador de servicios de salud se pueda inferir información adicional sobre el estado de salud del paciente y, en atención al riesgo de discriminación que pueda producirse en relación con este hecho , se podrán generar documentos o soportes genéricos a fin de evitar la identificación del centro de salud, siempre que este hecho no suponga una limitación de derechos fundamentales para el mismo interesado o para terceras personas.

3. Cuando resulte imprescindible para el reconocimiento de derechos del peticionario será posible incluir alguna de las informaciones siguientes:

    a. el servicio o especialidad en el que ha sido atendido el paciente;

    b. el diagnóstico derivado de la asistencia, y

    c. la fecha de ingreso del paciente, así como, en su caso, la fecha de alta.

4. Se podrá incluir cualquier otra información adicional si así lo autoriza el paciente o su representante.

5. Será altamente recomendable que las entidades establezcan protocolos para concretar, regular y estandarizar el contenido de los justificantes descritos en los apartados anteriores de manera que el personal siga unas instrucciones unánimes en el momento de elaborar estos justificantes.

Artículo 226-6. Protocolos de identificación de pacientes en la atención telefónica

Para la identificación positiva e inequívoca de los pacientes o usuarios de los servicios atendidos por vía telefónica, será necesario disponer de protocolos que permitan identificar claramente las personas atendidas por vía telefónica. Estos protocolos deberán basarse en mecanismos de solicitud de información al interesado que puedan ser comparados con los datos incorporados a las bases de datos y deberán evitar incorporar mecanismos basados en preguntas con respuestas de sí o no.

Artículo 226-7. Identificación de los perfiles de usuario

1. El responsable del tratamiento o el encargado documentará los diferentes perfiles de usuario que permiten el acceso a los sistemas de información e identificará los permisos de lectura, edición, modificación y demás que corresponda de acuerdo con las funciones y competencias de cada uno .

2. La documentación de perfiles a la que se refiere el apartado anterior deberá ser conocida, como mínimo, por el personal del departamento de gestión del personal y por el departamento de sistemas.

Artículo 226-8. Inventario de perfiles de usuario

1. El responsable del tratamiento o el encargado dispondrán de un inventario de usuarios con acceso al sistema que incluya su perfil, incluyendo la identificación de los programarios o bases de datos a los que pueda acceder cada perfil y los permisos de lectura, edición o eliminación otorgados a cada uno.

2. Se conservará una recopilación de todos los usuarios que han sido dados de alta en el sistema, así como los permisos vinculados al usuario, incluso cuando éstos estén suspendidos o dados de baja en el sistema.

3. El inventario identificará el histórico de usuarios que tengan la cuenta suspendida o inactiva. De manera anual se revisará el inventario de cuentas activas a fin de determinar si alguno de estos debe ser desactivado, a fin de evitar mantener cuentas activas que no respondan a ninguna necesidad de acceso a datos personales.

Artículo 226-9. Registro del historial de modificaciones

1. Siempre que sea posible, el programario utilizado para el tratamiento de la información médica de los interesados dispondrá de un mecanismo que permita

mantener un registro de cambios en el que conste el histórico de modificaciones hechas sobre la información, el usuario que ha hecho cada cambio y la fecha y hora de estos cambios.

Capítulo VII - Medidas para garantizar la exactitud y la autenticidad de los datos

Artículo 227-1. Protocolos de identificación de pacientes en el momento de la admisión

Las entidades deberán disponer de protocolos de identificación de pacientes que requieran la identificación positiva mediante comprobación de documentos oficiales con fotografía o mecanismo para identificar con seguridad la identidad del interesado, en especial cuando los datos obtenidos deban ser incorporadas a la historia clínica. El protocolo que regule la forma en que se han de identificar los pacientes deberá ser conocido por el personal que deba aplicar.

Artículo 227-2. Protocolos de identificación de pacientes en relación con la seguridad de los pacientes

Las entidades deberán disponer de protocolos de identificación de los pacientes adecuados a las situaciones en que se produzca esta identificación, y tendrán en consideración en todo momento tanto la privacidad de los interesados como los riesgos que puedan derivarse para la seguridad de los pacientes de un error en identificarlos. Estos protocolos o procedimientos resultarán especialmente pertinentes para los casos en que la identificación del paciente se haga en los momentos de desplazamiento, intervención y el suministro de medicación o alimentos, entre otros.

Artículo 227-3. Identificación de personas transgénero o transexuales

Las personas transgénero o transexuales se identificarán de manera que se respete la identificación del sexo con la que se identifica la persona a los efectos que el personal asistencial conozca la manera en la que deben relacionarse con el paciente. Sin embargo, mientras no se produzca la modificación formal del cambio de nombre a fin de hacerlo coincidente con la identificación de género de la persona, los datos se conservarán haciendo referencia a la identificación oficial de la persona de acuerdo con la normativa vigente.

Una vez se modifique legalmente el género de la persona y se modifique el nombre de acuerdo con la normativa vigente, se modificarán todos los datos de la persona a fin de hacerlos coincidir con su situación actual, a excepción de la historia clínica , en la que constará el mismo procedimiento de reasignación sexual y todas aquellas referencias al sexo biológico original que resulten relevantes para poder prestar asistencia sanitaria adecuada presente y futura.

Capítulo VIII - Medidas para garantizar la trazabilidad de los datos

Artículo 228-1. Registro de accesos

1. Los accesos a información médica de los interesados deberán quedar registrados de manera que se pueda determinar el usuario que ha accedido, la fecha y la hora en que ha tenido lugar.

2. El registro de los accesos a la información médica deberá tener en cuenta el usuario, la fecha y la hora del intento de acceso, aunque no se haya autorizado.

3. Cuando sea posible, los registros de acceso a la información identificarán si el acceso se ha hecho en el marco de una prestación de carácter asistencial o en el marco de la investigación en salud.

4. Los registros de acceso deberán ser custodiados por un periodo mínimo de tres años y deberá ser revisado periódicamente por un órgano unipersonal o colegiado al que se dote de competencias.

Artículo 228-2. Revisión del registro de accesos

1. Las revisiones periódicas del registro de accesos se harán mediante la revisión de una muestra aleatoria representativa de los accesos realizados en el período anterior a fin de validar su adecuación o justificación.

2. Habrá que someter a revisión los accesos denegados para validar que

    a. la denegación de acceso fue fruto de un error humano, y

    b. el usuario pudo, finalmente, acceder a los datos.

3. Se someterán a revisión los accesos producidos a la información de salud de las personas públicas atendidas en el período transcurrido desde la revisión anterior.

4. Se someterán a revisión los accesos producidos a la información de salud de los trabajadores, incluyendo los prestadores de servicios o relaciones análogas, del responsable del tratamiento atendidos en el período transcurrido desde la revisión anterior. Esta medida no será necesaria cuando los trabajadores dispongan de un mecanismo para conocer los accesos que se hayan producido sobre sus datos médicos.

Artículo 228-3. Acceso al registro de accesos

1. Todo interesado podrá acceder al registro de accesos a su información, por sí mismo oa través de un representante.

2. La información relativa al registro de accesos incluirá los perfiles de los usuarios que han accedido, la fecha, la hora y, en la medida de lo posible, la información obtenida.

3. El interesado tendrá derecho a solicitar que se revise la adecuación de los accesos sobre los que tenga sospechas o dudas de legitimidad. La respuesta a esta petición deberá ser lo antes posible dentro del plazo de tres meses.

4. Se identificarán, en el registro de accesos solicitado por el interesado, los profesionales que han accedido indebidamente, cuando el órgano de revisión de los accesos haya determinado, de forma indudable, el carácter indebido.

Capítulo IX - Medidas para garantizar la disponibilidad de los datos

Artículo 229-1. Copias de seguridad

1. Los sistemas informáticos utilizados para el tratamiento de datos personales deberán disponer de copias de seguridad que permitan garantizar la recuperación de los datos en caso de pérdida de la información.

2. Los soportes donde se ubiquen las copias de seguridad deberán disponer de las medidas físicas o lógicas adecuadas para garantizar que no se vean afectadas en caso de que el sistema de tratamiento de datos se vea afectado por ataques tipo ransomware u otros incidentes informáticos de tipo similar.

3. Los espacios donde se conserven los soportes que contengan las copias de seguridad estarán ubicados en una localización diferente de aquella donde estén ubicados los soportes que traten los datos originales.

4. Los espacios a los que se refiere el apartado anterior dispondrán de sistemas antiincendios. De acuerdo con los riesgos detectados, habrá que incorporar otras medidas de seguridad, en especial sobre la protección contra inundaciones u otros elementos ambientales que puedan poner en riesgo la información.

5. A los datos y soportes generados en la creación de las copias de seguridad se les aplicará las mismas medidas de seguridad que en los datos originales, sin perjuicio de que, por la misma naturaleza de copia de seguridad, se puedan aplicar medidas de seguridad adicionales.

Artículo 229-2. Abastecimiento eléctrico

1. Los sistemas automatizados de tratamiento de la información deberán disponer de mecanismos que garanticen el abastecimiento eléctrico en todo momento.

2. La contratación de los proveedores de energía deberá incorporar acuerdos de nivel de servicio que garanticen la recuperación del suministro de energía, en caso de incidencia, en un período de tiempo determinado. Los mecanismos de suministro de energía alternativos instalados por el responsable o encargado del tratamiento deberán garantizar el suministro eléctrico, como mínimo, durante este periodo.

Artículo 229-3. Aseguramiento de la conectividad

1. Los sistemas automatizados de tratamiento de la información deberán disponer de mecanismos que garanticen la disponibilidad de la información por medio de las conexiones en línea.

2. La contratación de los proveedores de servicios de conectividad, red y conexión deberá incorporar acuerdos de nivel de servicio que garanticen la disponibilidad de los datos y la conectividad con los servidores de manera que, en caso de incidencia, se minimice el impacto en los usuarios de los servicios de salud.

Artículo 229-4. Archivo de documentación física

Los espacios de custodia de la documentación física dispondrán de sistemas de cierre mecánico o sistemas análogos que impidan los accesos indebidos a la información. Los cierres deberán abarcar tanto las entradas al espacio físico donde se encuentra la documentación como el mobiliario donde esta está custodiada.

Artículo 229-5. Acceso a los centros de procesamiento de datos

1. El acceso a los centros de procesamiento de datos, tanto los principales como los auxiliares, deberán estar cerrados con mecanismos que impidan los accesos indebidos y se establecerán mecanismos de registro que identifiquen la persona que accede y la fecha y hora.

2. El responsable o encargado del tratamiento establecerá protocolos o instrucciones en los que se recojan las circunstancias y condiciones en las que se autorizará el acceso a los centros de procesamiento de datos a personas no autorizadas.

Artículo 229-6. Valoración del sistema

Para la valoración de los sistemas de tratamiento de datos, de acuerdo con lo dispuesto en el artículo 225-1 del presente Código de Conducta, se tendrá en especial consideración la disponibilidad de los datos de carácter de salud. A los efectos de valorar el nivel del sistema se considerará que el tiempo objetivo de recuperación de los datos de salud relativos a los pacientes se sitúa entre las 4 horas y las 24 horas.

Título III - Elementos para considerar en el análisis de riesgos y la evaluación de impacto en materia de protección de datos personales

Capítulo I - Elementos generales del tratamiento

Artículo 231-1. Formación del personal

Para la determinación de los riesgos del tratamiento será necesario considerar la formación en materia de protección de datos recibida por el personal de la organización y, en especial, por el personal interviniente en el tratamiento analizado. Se tendrá en consideración tanto el volumen de formación recibida como el tiempo transcurrido desde la última formación, y será obligatoria una formación cada dos años.

Artículo 231-2. Uso de formularios de campo libre

El uso de formularios de campo libre será considerado en los análisis de riesgo y evaluaciones de impacto como un elemento de acentuación de los riesgos derivados del tratamiento.

Artículo 231-3. Participación de los interesados en la valoración del riesgo

Para la determinación de los riesgos del tratamiento será necesario considerar la opinión de los interesados afectados por el tratamiento. La falta de participación de los interesados en el análisis de riesgo deberá ser motivada y considerada en la valoración del riesgo, y se incorporará como un elemento moderador al alza si la falta de participación de los interesados implica un elemento adicional de riesgo.

Capítulo II - Elementos relativos a la confidencialidad de los datos

Artículo 232-1. Identificación adecuada del receptor de la información

1. Para la determinación de los riesgos sobre la confidencialidad del tratamiento será necesario considerar los riesgos que puedan afectar a la confidencialidad de los datos de las personas por razón de la identificación incorrecta de la misma persona interesada o de las personas vinculadas.

2. En los casos en que la identificación de la persona interesada o de las personas que se vinculan se haga por medios telefónicos o telemáticos, se tendrán en cuenta los riesgos específicos que presentan estos canales de comunicación respecto de la correcta identificación del receptor de la información y sobre la confidencialidad de la información.

Capítulo III - Elementos relativos a la integridad de los datos

Artículo 233-1. Riesgos para la salud y la seguridad

1- Para la determinación de los riesgos del tratamiento se tendrán en consideración las consecuencias que pueden derivarse de una modificación de los datos no autorizada para la salud y seguridad del paciente.

2- En caso necesario, se valorará la efectividad de las medidas aplicadas o previstas que pretendan identificar la modificación indebida de los datos y restaurar los datos al estado original.

Capítulo IV - Elementos relativos a la exactitud y la autenticidad de los datos

Artículo 234-1. Afectación a la salud del interesado

Para la determinación de los riesgos del tratamiento se tendrán en consideración los efectos derivados de la identificación errónea del interesado en relación con la exactitud y autenticidad de los datos recogidos. A estos efectos se tendrá en cuenta la posibilidad de que se abran varias historias clínicas a un mismo paciente, así como la posibilidad de que se trate más de un paciente con una única identificación, incluso cuando los errores se deriven de la voluntad del propio interesado o de un tercero con su connivencia.

Artículo 234-2. Imposibilidad de acceder a procedimientos de carácter asistencial de la persona interesada

En el análisis de los riesgos de un tratamiento de datos se tendrán en cuenta los posibles efectos que una información carente de autenticidad puede tener sobre la posibilidad de acceso del interesado a procesos o procedimientos asistenciales concretos, o su inclusión en estudios o proyectos de investigación que puedan ser de interés de la persona interesada.

Capítulo V - Elementos relativos a la trazabilidad de los datos

Artículo 235-1. Registro de modificaciones

Para la determinación de los riesgos del tratamiento se tendrán en cuenta los riesgos derivados de la imposibilidad de conocer el alcance y origen de un acceso indebido y el riesgo de que las conductas de acceso indebido y alteración no autorizada de los datos queden sin ser descubiertas o, a pesar de descubrirse, no conlleven efectos disciplinarios adecuados para los responsables.

Capítulo VI - Elementos relativos a la disponibilidad de los datos

Artículo 236-1. Imposibilidad de acceder a los servicios asistenciales

En el análisis de los riesgos de los tratamientos será necesario identificar las situaciones en las que la falta de disponibilidad de los datos puede suponer la imposibilidad de prestar servicios de asistencia sanitaria a las personas interesadas.

Artículo 236-2. Afectación a la salud y daños físicos o psicológicos

En el análisis de los riesgos de los tratamientos será necesario identificar las situaciones en las que la falta de disponibilidad de los datos pueda suponer la aparición o agravación del estado de salud y de daños físicos o psicológicos derivados del retraso en la prestación de los servicios asistenciales.

Artículo 236-3. Pérdidas de tiempo

En el análisis de los riesgos de los tratamientos será necesario identificar las situaciones en las que la falta de disponibilidad de los datos suponga la existencia de desplazamientos innecesarios de las personas interesadas y la pérdida de tiempo por las dificultades en el seguimiento de la actividad habitual . Se tendrán en cuenta la capacidad del responsable del tratamiento de informar los interesados sobre las alteraciones en el servicio y la dispersión geográfica de la población de referencia y los tiempos de desplazamiento habituales al centro sanitario por los receptores de la asistencia sanitaria.

Capítulo VII - Medidas relativas a los capítulos anteriores

Artículo 237-1. Elementos relativos al riesgo de incumplimiento normativo

1. Los análisis de riesgo y evaluaciones de impacto sobre tratamientos de datos con fines asistenciales o sanitarios incorporarán el análisis de riesgo de incumplimiento normativo en relación con la normativa específica en materia de salud que tenga relación o impacto en la privacidad o el tratamiento de los datos personales.

2. Sin perjuicio de lo mencionado en el punto anterior, y sin carácter limitativo, se tendrán en consideración los siguientes elementos en el análisis de los riesgos de incumplimiento normativo:

    a) En cuanto al principio de minimización de los datos, habrá que velar por que la aplicación de este principio no suponga un riesgo para la seguridad del paciente.
    b) En relación con el deber de información, habrá que tener en cuenta las limitaciones o capacidades de las categorías de interesados de las que, previsiblemente, se traten los datos.

    c) Habrá que analizar el riesgo derivado de que los datos puedan ser utilizadas, por terceros, para proyectos de investigaciones o estudios de carácter científico o médico u otros fines de interés para estos terceros.

Capítulo VIII - Metodología aplicable en el análisis de riesgos y la evaluación de impacto

Artículo 238-1. Metodología

1. Los análisis de riesgos y evaluaciones de impacto llevadas a cabo por las entidades adheridas presentarán criterios objetivos de valoración de la probabilidad y gravedad de las situaciones de riesgo, a fin de permitir establecer criterios comparativos que permitan evaluar la evolución del riesgo en el tiempo y la afectación de las medidas aplicadas, los cambios en el estado de la técnica o los cambios en el contexto en que se hace el tratamiento.

2. Los análisis de riesgos y evaluaciones de impacto llevadas a cabo por las entidades adheridas presentarán situaciones de riesgo concretas propias de la

realidad asistencial. De estas situaciones se tendrán en cuenta, entre otras, las siguientes:

a. Categorías de interesados afectadas por el tratamiento de los datos, teniendo en especial consideración las capacidades cognitivas y de comprensión que puedan presentar.

b. Volumen de interesados previsiblemente afectos al tratamiento, tanto en número absoluto como en proporción al conjunto de población, tanto en general como en relación con las características de las categorías de interesados indicadas en el apartado anterior.

c. Volumen de categorías de datos tratados, en especial de datos de salud, de manera que se valore el nivel de precisión y conocimiento que podría adquirir un tercero que accede, de manera accidental o maliciosa, a estos datos sobre el estado de salud, diagnóstico o necesidades sanitarias de los interesados.

d. Las posibles finalidades previstas por el responsable del tratamiento a las que puede destinarse el tratamiento de los datos personales, en especial estudios sobre la mejora del servicio y estudios o investigaciones en materia de salud.

e. Las tecnologías aplicadas al tratamiento, teniendo en cuenta tanto el carácter innovador de la tecnología empleada como su carácter desactualizado. Habrá, asimismo, que evaluar las capacidades de los trabajadores y personal del responsable o de los encargados que traten los datos a través de los sistemas. Se deberán valorar los efectos sobre los riesgos que previsiblemente pueda tener la adopción de medidas relativas a la concienciación y la formación del personal en relación con el uso de las tecnologías aplicadas al tratamiento de los datos personales.

3. Las evaluaciones de impacto y los análisis de riesgo llevadas a cabo por el responsable del tratamiento tendrán en cuenta los riesgos derivados del contexto y entorno en el que se hace el tratamiento. En concreto, y sin efectos limitativos, se tendrá en cuenta lo siguiente:

a. Ámbito geográfico en el que tiene lugar el tratamiento o en el que se encuentran los interesados. Hay que tener en cuenta las posibilidades o dificultades que el ámbito geográfico y las infraestructuras del territorio puedan presentar respecto del tratamiento de los datos personales, en especial sobre la posibilidad de comunicarse con los interesados y la capacidad del Delegado de Protección de Datos de contactar con los interesados, en especial respecto de los medios telemáticos.

b. Elementos propios del entorno que puedan tener efectos en el tratamiento y la seguridad de los datos. En este sentido, se tendrán en

cuenta las características climáticas, es decir, las precipitaciones o más elementos que, por inundación, aislamiento u otras situaciones, puedan poner en riesgo la seguridad de los datos y, en especial, su disponibilidad.

Título IV - Medidas específicas para los tratamientos en el marco de la búsqueda e investigación en salud

Capítulo I - Uso de datos personales en búsqueda o investigación en salud

Artículo 241-1. Inclusión del ciclo de vida de los datos a los proyectos de investigación

La presentación de un proyecto de investigación por un investigador principal deberá incluir, en todo caso, una mención al ciclo de vida de los datos, en el que constarán las siguientes informaciones:

a) Forma de recogida de los datos, incluyendo el mecanismo de recogida de datos empleado cuando los datos se obtienen directamente del interesado o identificando las fuentes cuando los datos sean recogidos de terceros.

b) Forma de almacenamiento de los datos.

c) Tratamientos a los que, previsiblemente, se someterán los datos personales, identificando la forma en que los datos serán tratados, el programario utilizado y los tratamientos accesorios que pueden ser necesarios o adecuados para el correcto logro del proyecto de investigación.

d) Intervinientes en el tratamiento de los datos, identificando el perfil de los trabajadores y colaboradores que participarán en el tratamiento de los datos y los terceros que puedan participar en actividades de tratamiento como encargados del tratamiento.

e) Cesiones y comunicaciones de datos previstas.

f) Plazo de conservación de los datos y destino de estos una vez transcurrido este plazo.

Artículo 241-2. Minimización de los datos

1. Los datos tratados en el desarrollo de los proyectos de investigación serán los mínimos necesarios para alcanzar, con garantías suficientes sobre la validez de los resultados, los objetivos del proyecto de investigación. Cuando los datos se obtengan de fuentes o bases de datos donde conste más información de la necesaria en relación con el objetivo del proyecto de investigación, se generará una base de datos específica que recoja únicamente la información que resulte necesaria para el equipo investigador. Esta base de datos la generará a partir de la fuente original un equipo separado técnica y funcionalmente del equipo

investigador, que deberá asumir un compromiso expreso de no entregar al equipo investigador ninguna información adicional a aquella necesaria para el estudio.

2. A los efectos de generar las bases de datos con información mínima a las que se refiere el apartado anterior se podrán emplear soluciones tecnológicas que garanticen que el equipo investigador accede únicamente a los datos necesarios para el desarrollo del proyecto de investigación. Las soluciones tecnológicas aplicadas deberán garantizar la separación técnica y funcional entre el equipo investigador y el equipo que tenga el control sobre el diseño o funcionamiento de estas herramientas y sobre la creación de los conjuntos de datos necesarios para la investigación.

Capítulo II - Medidas de salvaguarda de los derechos de los interesados

Artículo 242-1. Registro de los proyectos de investigación

1. Sin perjuicio del mecanismo utilizado para dar cumplimiento al deber de información a los interesados, las entidades que desarrollen actividades de investigación pondrán a disposición de los interesados, por medios electrónicos, una lista actualizada de los proyectos de investigación que se estén llevando a cabo.

2. El registro al que se refiere el apartado anterior identificará el proyecto de investigación, la especialidad médica o investigadora a la que está vinculado, la fuente de la que se obtienen los datos y si los datos se emplean de manera anonimizada o seudonimizada

3. El registro incluirá información sobre el tratamiento de los datos personales, cuando proceda, o la indicación sobre dónde se puede consultar esta información, que deberá estar disponible por medios telemáticos.

Capítulo III - Conservación de los datos en el marco de la búsqueda o investigación en salud

Artículo 243-1. Conservación de los datos

1. El plazo de conservación de los datos en el marco de los tratamientos vinculados a la búsqueda o investigación en salud estará definido, sin perjuicio de lo que establezca la normativa aplicable, por el plazo establecido en el ciclo de vida de los datos al que se refiere el artículo 241 -1 del presente Código de Conducta.

2. El plazo de conservación de los datos se entenderá cumplido cuando, en el marco de los proyectos de búsqueda e investigación en salud con datos seudonimizados, se elimine la información adicional que permite la

reidentificación de las personas físicas, de manera que ya no sea posible esta reidentificación.

Disposición Final - Entrada en vigor

Las disposiciones establecidas en el presente Código de Conducta para el tratamiento de datos personales en el ámbito sanitario del Consorcio de Salud y de Atención Social de Cataluña entrarán en vigor desde el momento en que este Código sea aprobado y publicado por la Autoridad Catalana de protección de Datos y se encuentre publicado en la web del Consorcio de Salud y de Atención Social de Cataluña.

Codi de Conducta

Consorci de Salut i Social de Catalunya