Informe sobre la perspectiva ética en la interoperabilidad de datos entre el sistema social y el sistema sanitario

Informe sobre la perspectiva ética en la interoperabilidad de datos entre el sistema social y el sistema sanitario

Junio 2025

Dirección Atención Sociosanitaria

Departamento de Salud

Gobierno Vasco

Comisión Sociosanitaria de Comités de Ética de Euskadi

Estrategia de Atención Sociosanitaria de Euskadi 2021-2024

Índice

Introducción y contextualización

En los últimos años el concepto de interoperabilidad en los sistemas social y sanitario está adquiriendo cada vez mayor importancia debido, en buena medida, a los nuevos requisitos que los sistemas de atención deben afrontar para poder prestar su servicio de forma efectiva, eficiente y sostenible; los cambios demográficos, la movilidad de la ciudadanía y la equidad en el acceso son los más relevantes.

La interoperabilidad entre los sistemas de información social y sanitario es un ámbito de gran complejidad tanto desde el punto de vista técnico como organizativo. A pesar de su relevancia para la integración de los servicios de salud y atención social, su desarrollo e implementación sigue siendo limitado y heterogéneo en las diferentes administraciones y territorios. No es suficiente que dos sistemas de información se intercambien datos que más o menos puedan entender, sino que es necesario además establecer enlaces o relaciones en varios niveles distintos de las organizaciones.

Los avances tecnológicos ayudan en la optimización de los procesos y aumentan la eficiencia en la atención a las personas, en la reducción de costes y optimización de los recursos, permitiendo a los y las profesionales centrarse en tareas de mayor valor añadido; **sin embargo, han suscitado preocupaciones éticas que plantean importantes interrogantes sobre el futuro de la humanidad y el equilibrio entre el progreso y la responsabilidad.** La privacidad de la información, la desigualdad en el acceso y manejo de las tecnologías y sus avances, la autonomía y responsabilidad en la toma de decisiones, los monopolios tecnológicos y de la información, y la monetización de los datos de las personas son algunas de estas cuestiones.

Si bien existen iniciativas en curso y experiencias que buscan avanzar en este proceso, no se han identificado documentos específicos que aborden esta cuestión desde una perspectiva ética.

Propósito del documento

La Comisión Sociosanitaria de Comités de Ética de Euskadi (CSSCEE), es un órgano de carácter interdisciplinar, adscrito al Consejo Vasco de Atención Sociosanitaria, creado para coordinar a los diferentes Comités de Ética de Intervención Social y a los Comités de Ética Asistencial del ámbito sanitario, de los tres Territorios Históricos de la Comunidad Autónoma de Euskadi.

Es un órgano consultivo, que, entre otras funciones, elabora informes y dictámenes de contenido ético en materia social, sanitaria y sociosanitaria a petición de instituciones como los departamentos del Gobierno Vasco competentes en materia de políticas sociales y de salud, las diputaciones forales y Eudel/Asociación de Municipios Vascos. Su autoridad es únicamente moral, y tiene autonomía en su funcionamiento.

El presente documento se genera como resultado de una petición desde la Dirección de Atención Sociosanitaria (DASS), dependiente del Departamento de Salud del Gobierno Vasco, en el marco del impulso a la interoperabilidad sociosanitaria entre los sistemas sanitarios y de atención social.

Se trata de incorporar un enfoque ético, abierto y basado en los derechos humanos en el uso de datos sobre salud y atención social en la Comunidad Autónoma Vasca (CAV), para lograr un ecosistema de salud y cuidado confiable y, donde los datos se compartan, gestionen y se almacenen de forma segura, coherente, eficiente y transparente.

A la hora de la elaborar el documento, el guion que se ha seguido ha tratado de identificar los principios y valores éticos que deben ser respetados para que la interoperabilidad se lleve a cabo de forma correcta desde una perspectiva ética; las recomendaciones que se exponen a continuación son acciones a tener en cuenta con el fin de evitar que dichos principios y valores sean vulnerados.

Definición de interoperabilidad y finalidad de esta

Entendemos por interoperabilidad la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. El tratamiento de datos personales debe estar concebido para mejorar la atención y cuidados de la ciudadanía.

En el contexto de la asistencia sociosanitaria, se podría considerar la interoperabilidad como **la capacidad de los sistemas sanitarios y de servicios sociales de intercambiar información de forma fluida y controlada, utilizar la información intercambiada de forma significativa y poseer la capacidad de trabajar juntos dentro y fuera de los límites organizativos con el objetivo de proporcionar una mejor atención a las personas.**

Cuando hablamos del uso significativo de la información nos referimos a la capacidad de los sistemas electrónicos de asistencia sanitaria y social para mejorar la calidad, la seguridad, la eficiencia de las prestaciones y reducir disparidades implicando a las personas (y en caso necesario a sus familias) en el proceso asistencial, de esta manera la información intercambiada mejorará la coordinación asistencial, la salud pública y de la población, manteniendo la privacidad y la seguridad de la información social y sanitaria de las personas atendidas.

La interoperabilidad en el intercambio de datos en el ámbito sociosanitario tiene muchas ventajas como, por ejemplo:

- La mejora de la comunicación. La interoperabilidad facilita la colaboración, la interacción y el intercambio de información necesaria en el contexto asistencial.
- La reutilización de la información.
- La garantía de que se transmite la información con el significado correcto.
- La reducción de errores.

Pero también tiene el riesgo de poner en peligro la confidencialidad exigible a cualquier acto profesional por lo que supone de pérdida de confianza y pérdida de control por parte de la persona de quién tiene su información.

La finalidad de la interoperabilidad es integrar los sistemas de información para compartir datos sociales y sanitarios y facilitar la toma de decisiones en la atención de la ciudadanía, una atención sociosanitaria coordinada e integral que ponga en el centro de sus actuaciones a las personas, manteniendo la seguridad y la confidencialidad de las mismas.

Fundamentación legal

Entendiendo la interoperabilidad como la acabamos de definir, **aunque no es solo tratamiento de datos, sí tiene un componente fundamental en el tratamiento de datos** por lo que, desde una perspectiva legal, sea cual sea el procedimiento, sistema y organización que se adopte para lograr la interoperabilidad en la asistencia sociosanitaria, deberá cumplir con la legislación vigente a nivel europeo, estatal y, en su caso, autonómico en esta materia.

En esta línea, sin excluir otra legislación que también pueda ser de aplicación, las principales normas que se deben tener en cuenta respecto del tratamiento de datos personales son:

- Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE, 6 de diciembre de 2018)

De estas normas, y principalmente de las consideraciones previas al articulado del Reglamento europeo de 2016, se extraen una serie de principios que han de respetarse en cualquier sistema que se establezca para la interoperabilidad.

Ya en la primera consideración se establece que la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental, y así está recogido en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea.

El tratamiento de datos personales debe orientarse al servicio de la humanidad. La evolución tecnológica y la globalización, tan rápidas en los últimos tiempos, plantean nuevos retos para la protección de los datos personales que requieren respuestas respetuosas con esta protección.

Las personas físicas deben tener el control de sus propios datos personales. En este sentido, la consideración 32 del Reglamento europeo dice que *"el consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca de la persona interesada de aceptar el tratamiento de datos de carácter personal que le conciernen"*, y que *"el consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos."*

Dado que este informe se refiere a la interoperabilidad sociosanitaria, interesa también recordar que *"entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud de la persona interesada que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia"* (consideración 35 del Reglamento europeo).

Teniendo en cuenta el objeto de este informe, es importante recordar que la Consideración 42 del Reglamento europeo nos dice que cuanto el consentimiento se presta *"en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que la persona interesada es consciente del hecho de que da su consentimiento y de la medida en que lo hace. Para que el consentimiento sea informado, la persona interesada debe conocer como mínimo la identidad del/de la responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando la persona interesada no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno."*

"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro…Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida… Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios." (Consideración 39 del Reglamento europeo).

Por lo que se refiere a la licitud, y siguiendo lo que se recoge en la Consideración 40 del Reglamento europeo, *"los datos personales deben ser tratados con el consentimiento de la persona interesada o sobre alguna otra base legítima establecida conforme a Derecho"* que debe ser clara y precisa y su aplicación previsible para sus destinatarios.

"El tratamiento de categorías especiales de datos personales sin el consentimiento del interesado puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas… Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines." (Consideración 54 del Reglamento europeo)

"En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado." (Consideración 69).

Además de este derecho de oposición, reconocido por el Reglamento europeo de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe tenerse en cuenta también en la gestión de la interoperabilidad sociosanitaria el derecho de autoexclusión del tratamiento de datos de salud electrónicos personales para uso secundario (el tratamiento de datos de salud

electrónicos para fines distintos de los iniciales para los que se recogieron o produjeron) regulado en el artículo 71 del Reglamento relativo al Espacio Europeo de Datos de Salud: *"1. Las personas físicas tendrán derecho de autoexclusión, en cualquier momento y sin necesidad de exponer los motivos [...] El ejercicio de ese derecho será revocable. […] 2. Los Estados miembros proporcionarán un mecanismo de autoexclusión accesible y de fácil comprensión para el ejercicio del derecho establecido en el apartado 1, con arreglo al cual las personas físicas podrán manifestar expresamente que no desean que sus datos de salud electrónicos personales sean tratados para uso secundario."*

Es posible la excepción a este derecho siempre y cuando se regule en la legislación nacional de cada Estado miembro para supuestos que cumplan una serie de requisitos establecidos por la norma europea, lo que en la práctica exigirá el análisis de cada supuesto en particular. Cómo y por quién haya de hacerse este análisis no se establece en la normativa europea, pero, como ha dicho el *"Informe del Comité de Bioética de España sobre la supervisión ética del tratamiento de datos en el contexto del Espacio Europeo De Datos De Salud (EEDS) 2025", "conviene tener presente que es el tipo de cuestión que ha de quedar bien aclarada."* Siguiendo la recomendación de este informe, debería ser *"una entidad supervisora con capacidad para proveer al organismo administrativo correspondiente de recomendaciones desde la ética"* quien debería asegurar que la solicitud *"para obtener un permiso que habilite el tratamiento de datos sujetos a un derecho de autoexclusión"* contiene las garantías suficientes proteger los derechos fundamentales y los datos personales de las personas físicas.

El análisis desde un punto de vista legal del sistema, procedimiento u organización que se establezca para lograr la interoperabilidad sociosanitaria se podrá realizar por quien corresponda una vez que se tenga un proyecto más concreto de cómo va a llevarse a cabo, analizando si los mecanismos que se establezcan cumplen o no con la legislación en materia de protección de datos.

En este informe, con carácter previo, solo se puede recordar cuál es el marco legal y cuáles son los principales principios que han de respetarse y tenerse en cuenta a la hora de diseñar el sistema.

Fundamentación ética

La **ética en las organizaciones** se fundamenta en un conjunto de valores y normas que guían sus actuaciones, integrándose en la cultura organizativa para asegurar la coherencia, la confianza, la justicia social y el respeto a los derechos humanos, respondiendo así a las necesidades sociales y promoviendo el bienestar colectivo. Por su parte, la **ética centrada en la persona** sitúa a cada individuo como sujeto único de derechos, dignidad y autonomía, priorizando sus preferencias, su participación activa y el respeto a su identidad en la toma de decisiones y en la configuración de su propio proyecto de vida.

Ambas perspectivas confluyen en la necesidad de proporcionar una atención integral y personalizada, especialmente relevante para personas en situación de dependencia o vulnerabilidad, cuyo bienestar depende de la coordinación efectiva entre múltiples agentes y servicios. Para que este enfoque sea real y efectivo, resulta imprescindible que las organizaciones y profesionales compartan información relevante de manera responsable, segura y respetuosa, lo que exige **una interoperabilidad basada en principios éticos** como la confidencialidad, el consentimiento informado y la equidad en el acceso a los servicios.

La ética debe ser entendida como un **paradigma de buen diseño de los sistemas de información.** Habitualmente los sistemas se diseñan para cumplir una automatización productiva, y carecen de un enfoque centrado en la persona y por tanto en la perspectiva ética.

A pesar de las numerosas ventajas de la interoperabilidad de los sistemas electrónicos de asistencia sanitaria, social y sociosanitaria, la mayoría de estos sistemas electrónicos no son totalmente interoperables, sobre todo por cuestiones éticas, como la seguridad de la información de las personas, la privacidad, el consentimiento, la confidencialidad, la propiedad de la información de los pacientes y la desidentificación de la información, entre otras.

Habitualmente los sistemas se diseñan para cumplir una automatización productiva, y carecen de un enfoque centrado en la persona y por tanto en la perspectiva ética.

La gestión responsable de la información requiere una visión integral que contemple las distintas realidades y necesidades de todos los agentes involucrados. Por ello, proponemos una fundamentación ética basada en principios y valores organizados en tres dimensiones clave que son las siguientes y cada una de las cuales se desarrollan en detalle en este apartado:

- las personas atendidas, quienes merecen la máxima protección y respeto de su privacidad;
- los y las profesionales, responsables de un manejo ético y diligente de los datos;
- y el uso de los datos, que debe orientarse siempre al interés legítimo, la transparencia y la seguridad. Esta estructura nos permitirá abordar de manera específica los retos y compromisos éticos que surgen en cada ámbito, garantizando un tratamiento de los datos justo, seguro y alineado con los derechos fundamentales.

Consideraciones éticas relativas a las personas atendidas

Aquí se recogen las consideraciones éticas clave relacionadas con los derechos de las personas atendidas, poniendo el foco en su autonomía, privacidad y protección frente a posibles daños.

Respeto a la autonomía de la persona

La autonomía es el derecho de la persona a determinar su propia atención sanitaria y sociosanitaria. Por lo tanto, las personas deben tener derecho a esta información también cuando la información es creada y gestionada por profesionales. Así, las personas deben ser plenamente conscientes antes de que su información se intercambie entre diversos sistemas de atención sociosanitaria. Las personas también deben tener la oportunidad de dar su pleno consentimiento para el intercambio de la información. De lo contrario, la confianza de las personas atendidas en los y las profesionales podría verse amenazada, lo que les impediría revelar información sensible necesaria para una atención adecuada.

El respeto de la autonomía permite a las personas tener cierto grado de control sobre su información durante el intercambio de información entre los y las profesionales sociosanitarios. De este modo, se evitará la divulgación no autorizada de información especialmente sensible. La persona puede dar autorización para la interoperabilidad de determinados datos y no de otros.

Privacidad

La privacidad implica la capacidad de una persona de controlar la información sobre sí misma.

En todo caso, en el ámbito que estamos desarrollando, la privacidad también puede considerarse como la capacidad de proteger la información de las personas frente a accesos no autorizados y a la divulgación, es decir, garantizar la seguridad.

Licitud, lealtad y transparencia

En relación con la persona interesada. Es esencial fomentar la transparencia y la rendición de cuentas en el uso de datos, garantizando que las personas usuarias comprendan cómo se recopilan, almacenan y utilizan sus datos (deben ser procesos trazables) y tengan control sobre su información personal. Para ello, la información debe ser clara, accesible y de lectura fácil.

Prevención del daño

La interoperabilidad de los datos no debería provocar daños (o agravar los existentes) ni perjudicar de cualquier otro modo a las personas (por ejemplo, en relación a ámbitos públicos como derecho a prestaciones, procedimientos legales). Los datos del ámbito privado (sanitario o servicios sociales) no deben en ningún caso ser conocidos y utilizados para cuestiones ajenas a la atención y cuidado de las personas. Esto conlleva a la protección de la dignidad humana, así como de la integridad física y mental. Los sistemas que utilicemos deben ir alineados con la protección de los derechos humanos.

Aspecto éticos relacionados con los y las profesionales

Este apartado aborda aspectos éticos fundamentales que deben guiar la actuación de los y las profesionales en el uso de datos, destacando su responsabilidad, compromiso y respeto hacia la confidencialidad y la protección de derechos.

Confidencialidad

La confidencialidad se relaciona con el compromiso de profesionales y organización de controlar la información, de poner los datos a disposición únicamente de las personas o procesos autorizados.

Los sistemas de atención sanitaria y sociosanitaria son vulnerables a los retos de privacidad y confidencialidad debido a la naturaleza de la información que adquiere, almacena y transmite.

Profesionalismo

El profesionalismo sociosanitario implica una serie de valores, habilidades y compromisos esenciales para la calidad de la atención de las personas. Estos valores y habilidades se enfocan en el bienestar de la persona, la integridad profesional y la responsabilidad con la sociedad.

En el ámbito del uso de sistemas electrónicos interoperables implica respetar la confidencialidad, garantizar la disponibilidad, precisión, integridad, seguridad y transparencia de los datos de salud de manera responsable. Asimismo, supone una utilización equitativa de los mismos, no discriminatoria y respetuosa de la privacidad, evitando cualquier uso que pueda generar un daño o un beneficio desproporcionado para algunos/as. Para ello es necesario el respeto de los y las profesionales al principio de proporcionalidad entre medios y fines y estudiar cuidadosamente cómo alcanzar un equilibrio entre los diferentes intereses y objetivos.

Responsabilidad proactiva

Todas aquellas personas que se encuentran implicadas en un tratamiento de los datos a lo largo de todo su ciclo vital deben ser conscientes de su responsabilidad para que se cumplan los principios anteriormente citados, a fin de garantizar el derecho fundamental a la protección de los datos, por lo que el factor de concienciación y formación es fundamental para llevar a cabo esta proactividad.

Principios clave del uso de los datos

A continuación se presentan los principios clave que deben guiar el uso de los datos en contextos de interoperabilidad, con el fin de garantizar su seguridad, integridad y uso responsable.

Seguridad

La recopilación de datos debe realizarse de manera transparente y ética, con el consentimiento informado de los usuarios y de acuerdo con las leyes y regulaciones de privacidad aplicables. Es esencial que los datos se manejen de manera segura y se protejan contra el acceso no autorizado, el uso indebido o la destrucción no autorizada de los datos.

Confianza o Confiabilidad

Los sistemas deben de tener la capacidad de resistir acciones ilícitas o malintencionadas que comprometan la autenticidad, integridad y confidencialidad de los datos y pongan en riesgo la confianza.

Integridad

Es necesario adoptar las medidas técnicas u organizativas adecuadas que impidan la pérdida, destrucción o daño accidental de los datos.

Minimización

La interoperabilidad debe limitar el tratamiento de datos a lo estrictamente necesario para el cumplimiento de los fines, y debe evitar el uso de información innecesaria.

Limitación de la finalidad

Recogidos con fines determinados, no serán ulteriormente tratados de manera incompatible con otros fines.

La limitación de finalidad en la interoperabilidad de datos significa que los datos, una vez recogidos para un propósito específico, no pueden ser tratados de forma incompatible con ese fin original. En la práctica, implica que la interoperabilidad (el intercambio y uso de datos entre sistemas) debe estar regulada para garantizar que los datos no sean usados para fines no autorizados por la persona que ha otorgado el consentimiento o que puedan comprometer la privacidad de los datos

La limitación de finalidad garantiza que:

- Los datos no son utilizados para fines distintos a los que fueron recolectados.
- La interoperabilidad no se utiliza para obtener información o acceder a datos de manera no autorizada.
- La privacidad de los ciudadanos se respeta, ya que se limita el tratamiento de datos personales.

El principio de limitación de la finalidad en la interoperabilidad de datos debe tomar en cuenta:

- Los fines específicos y legítimos de dicha interoperabilidad, es decir, los datos solo pueden ser tratados para los fines para los que fueron recogidos y con el consentimiento del titular de los datos.
- La compatibilidad, de manera que se garantice que el intercambio de datos no afecte negativamente los fines originales para los que se recolectaron.

Exactitud

Los datos deben ser correctos y actualizados, debiendo adoptarse todas las medidas razonables para que se supriman o rectifiquen los datos que sean inexactos.

Limitación del plazo de conservación

La interoperabilidad debe asegurar que los datos no se conserven más tiempo del que sea necesario para el cumplimiento de los fines, y que sean suprimidos cuando ya no sean necesarios.

Selección y elección

Se puede dar autorización para la interoperabilidad de determinados datos y no de otros, bajo la premisa de seleccionar y elegir los datos relevantes y necesarios para un propósito específico siempre que sean interoperables y que puedan ser utilizados por los sistemas o procesos que los requieren.

Recomendaciones

A modo de conclusión de este informe, a continuación, se recoge una serie de recomendaciones para ayudar a la incorporación de la dimensión ética en el desarrollo e implementación de los sistemas de interoperabilidad. Antes, por su relevancia, se hace referencia al consentimiento informado como elemento esencial para que la persona tome decisiones autónomas sobre su atención.

El **consentimiento informado** es el procedimiento que da prueba de que se ha pedido a la persona autorización para compartir información que le afecta y ha consentido el acceso a la misma. Implica información sobre el contenido a compartir, la/s persona/s que van a acceder y la finalidad de esta. Tiene que ver con la autonomía personal y la toma de decisiones. Dicho consentimiento deberá ser otorgado por la propia persona o, en su defecto, quien le represente. Deberá ser bidireccional, que contenga información detallada de los datos que se van a compartir y que comparta un enunciado base, pero que no sea genérico, si no adaptado a cada caso, especialmente importante en personas en situaciones de vulnerabilidad.

A continuación las **recomendaciones para incorporar la ética en la interoperabilidad sociosanitaria:**

- Establecer mecanismos de detección, prevención y seguimiento de los riesgos que afectan a la seguridad y a los derechos fundamentales, garantizando su control técnico.
- Formación, capacitación y concienciación sobre asuntos relevantes, entre otros: el proceso de información y obtención del consentimiento informado; el uso adecuado de la herramienta que se establezca; el derecho a la integrad y deber de confidencialidad; y la adecuación y pertinencia de la información a compartir respecto al caso concreto.
- Educación y sensibilización sobre la importancia de incluir la perspectiva ética en la interoperabilidad de datos.
- Elaborar protocolos y procedimientos de manera que todos los y las profesionales puedan garantizar a la persona que los y las profesionales que intervienen guardarán la confidencialidad y cumplirán con la obligación de secreto profesional.
- Disponer de guías prácticas y marcos éticos para orientar las decisiones públicas, desarrollo de algoritmos, etc.
- Implementar medidas de seguridad robustas, como el cifrado de datos y el anonimato, y establecer políticas claras de retención y eliminación de información.
- Establecer un sistema trazabilidad para que se pueda saber quién, cuándo y para qué ha accedido a los datos.

- Elaborar un código ético que comprometa en su cumplimiento a las personas profesionales y a las direcciones de las organizaciones.

- Establecer una buena comunicación entre las organizaciones y profesionales de los sistemas sanitarios, sociales y socio sanitarios más allá de los canales de interoperabilidad.

- Implementar mecanismos de monitorización y evaluación continua para identificar y corregir problemas a medida que surgen.

- Establecer indicadores de uso que puedan darnos una idea de qué casos se utiliza más, qué datos se intercambian, motivo de intercambio de datos, qué ámbito, social y/o sanitario, solicita más información, …

- Solidez técnica de los sistemas, de manera que estén protegidos y sean resistentes a los ataques y den sensación de seguridad.

- Establecer un compromiso por parte de las organizaciones y sistemas en el cumplimiento de las recomendaciones que se señalan.

Bibliografía

Decreto 150/2022, de 7 de diciembre, de la gobernanza sociosanitaria en Euskadi

Informe del Comité de Bioética de España sobre la supervisión ética del tratamiento de datos en el contexto del espacio europeo de datos de salud (EDDS). 2025. Comité de Bioética de España

La protección de datos y la interoperabilidad en el ámbito sanitario: dos realidades inseparables. Muñoz Fernández, L. Gallego Riestra, S. *Volumen 29 número 2. Julio-diciembre 2019. ESTUDIOS*

Ganiat, IO. Olusola, OJ. Communications on Applied Electronics (2015) Ethical issues in interoperability of electronic healthcare systems.

Código ético para el desarrollo, uso e implementación de Inteligencia Artificial en Euskadi. BAIC (Basque Artificial Intelligence Center)

Goikoetxea, M. (2023). "Cuidados integrados de larga duración desde el modelo ACP - Perspectiva ética". Universidad de Deusto. Disponible en: https://serviciossociales.jcyl.es/web/jcyl/binarios/334/51/Cuidados%20integrados%20de%20larga%20duraci%C3%B3n%20desde%20el%20modelo%20ACP%20-Perspectiva%20ETICA.pdf

Bioética Andalucía. "Ética y gestión de la organización sanitaria". Disponible en: https://www.bioetica-andalucia.es/4-etica-y-gestion-de-la-organizacion-sanitaria/

Morcillo, J. M. (2024). "Los retos éticos de profesionales y pacientes en el sector sociosanitario". Revista UNIR de Ciencias Sociales. Universidad Internacional de La Rioja. Disponible en: https://www.unir.net/revista/ciencias-sociales/los-retos-eticos-de-profesionales-y-pacientes-en-el-sector-sociosanitario/

Olympia Anastasiadou, Panagiotis Mpogiatzidis, Pantelis Angelidis (2024) Ethical Issues Regarding the Digitalization and Interoperability of Health Services. Journal of Biotechnology & Bioinformatics Research. SRC/JBBR-209.