RECOMENDACIONES PARA EL USO DE DATOS EN SALUD

TRATAMIENTO LEGAL Y ÉTICO DE LOS DATOS SANITARIOS INDIVIDUALES Y MASIVOS EN SALUD

Observatorio de Salud de la Facultad de Derecho de la UBA

Dirección Académica: Dra. Marisa Aizenberg

MESA DE DIÁLOGO

Contenido del documento **Pág.**

Encuadre

El Observatorio de Salud de la Facultad de Derecho de la Universidad de Buenos Aires fue creado hace una década con el objetivo de contribuir con su tarea a la mejora de políticas y servicios sanitarios y fortalecer una mayor equidad y acceso a la salud. Así, se ha constituido en un espacio para la creación de consensos y generación de propuestas orientadas a fortalecer el funcionamiento del sistema de salud argentino.

Las nuevas tecnologías junto al manejo de datos masivos y grandes volúmenes de información sensible sobre salud plantean interrogantes y dilemas sanitarios, jurídicos y éticos que requieren de un abordaje interdisciplinario y constituyen una oportunidad para establecer pautas para el fortalecimiento de los derechos ciudadanos en clave sanitaria.

Este ha sido el espíritu de la convocatoria a la conformación de una Mesa de Diálogo desde el ámbito académico, para permitir reflexiones y debates informados, con el objetivo de ofrecer una visión intersectorial donde surjan recomendaciones sobre estos importantes cambios que impactan al sistema sanitario. Así, gracias a la participación y compromiso de un grupo de organismos e instituciones se ha consensuado el presente documento que contiene las **Recomendaciones para el Tratamiento Legal y Ético de los Datos Individuales y Masivos en Salud**.

Justificación.

La masificación de los datos, su valor en una sociedad globalizada, junto al uso de tecnología ha posibilitado el acceso, sin control adecuado, a información de índole personal que puede importar la vulneración e intromisión en una esfera de intimidad y privacidad no consentida por las personas.

Los datos se erigen en el oro de este siglo y conforman un preciado activo en materia de gobernanza y negocios.

A la par de las bases privadas de datos masivos se suman las bases públicas mediante las cuales los gobiernos centralizan repositorios de información personal y biométrica (huellas y rostros digitalizados), que puede interoperar y entrecruzar datos con sistemas de vigilancia y seguridad para individualizar a los individuos mediante técnicas de reconocimiento facial o facilitar su geolocalización y seguimiento, por caso, todo ello con potenciales consecuencias sobre los derechos fundamentales.

En el área de salud, el análisis de grandes volúmenes de datos (Big Data) ofrece un futuro promisorio para predecir tendencias y prevenir enfermedades o epidemias. Mediante múltiples fuentes de registros digitales se obtienen grandes y variados volúmenes de datos y a gran velocidad.

En Argentina la protección de datos personales constituye un derecho fundamental, garantizado por la Constitución Nacional (art. 43), regulado por la Ley Nº 25.326. Aún así, la relevancia de los temas involucrados requiere que los actores implicados en todo el proceso, desde informáticos hasta gobierno, desde pacientes, médicos hasta universidades se comprometan con un proyecto de gobernanza de salud digital que pueda enfrentar los desafíos planteados, desde diversas perspectivas compartidas.

Es por ello que el Observatorio de Salud ha convocado a una Mesa de Diálogo que luego de fecundas reuniones consensuó las siguientes Recomendaciones.

Recomendaciones.

I. GENERALES.

La innovación tecnológica ha impactado fuertemente en el sector sanitario. Hemos atravesado la tradición estática (historia clínica, resultados de laboratorio, imágenes) para ingresar a otra más dinámica, con enormes conjuntos de datos provenientes de múltiples fuentes (genómica, genética, registros clínicos electrónicos, redes sociales, monitorización de pacientes en tiempo real, aplicaciones móviles). Ellos se combinan a través de avanzadas técnicas de análisis utilizando algoritmos matemáticos, inteligencia artificial, machine learning, modelos estadísticos, redes neuronales, procesamiento de lenguaje natural y otras metodologías, que permiten establecer técnicas analíticas predictivas a partir de relaciones y determinar tendencias, patrones y comportamientos sanitarios individuales o poblacionales.

En función de ello **se recomienda**

1. Propiciar el desarrollo de políticas públicas tendientes a la protección de los datos personales en salud que aseguren los derechos fundamentales.
2. Promover la adecuación de los marcos legales y prácticas éticas, en el contexto de una estrategia de salud digital nacional y regional que provea un sistema de derechos, obligaciones, responsabilidades y controles adecuados, junto a salvaguardas eficaces para la protección de derechos, que sean flexibles y permitan el desarrollo de la innovación.
3. Entender que la protección de los datos sanitarios comprende tanto los registros médicos y administrativos nominalizados como sus documentos complementarios, debiendo asegurarse su integridad, autenticidad, inalterabilidad, perdurabilidad, disponibilidad en todo momento y que existan mecanismos de recuperación de los datos de salud almacenados.
4. Introducir oportunidades de mejora en la coordinación y articulación de los subsistemas sanitarios a través del uso adecuado de datos relativos a salud.
5. Establecer mecanismos de contralor, homologación y/o certificación, según corresponda para las aplicaciones y empresas de desarrollo informático vinculadas a la recolección automática o programada de datos sanitarios.

II. CIUDADANÍA SANITARIA

Existen en nuestro país marcos regulatorios de protección de datos personales que permiten a los individuos ejercer cierto control sobre aquellos datos de carácter personal que se encuentran en bases de titularidad de terceros, sean públicas o privadas, saber qué datos se almacenan y quién procede a su recolección y tratamiento, para qué fines, ello con el objeto de autorizar u oponerse a su recolección, posesión, tratamiento y uso.

En Argentina la protección de datos personales constituye un derecho fundamental, garantizado por la Constitución Nacional, cuyo artículo 43 otorga a toda persona la posibilidad de interponer una acción de "habeas data" para tomar conocimiento de los datos que consten en registros o bancos de datos públicos o privados –destinados a proveer informes-, así como su finalidad y, en caso de falsedad o discriminación, poder exigir su supresión, rectificación, confidencialidad o actualización.

Este derecho conocido como autodeterminación informativa ofrece la potestad de controlar la información personal, intima o no, como respuesta a los avances tecnológicos que invaden zonas de privacidad y pueden vulnerar la identidad, dignidad, libertad y otros derechos e intereses personales.

Por su parte, el objeto de la Ley Nº 25.326 es la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre las mismas se registre.

En función de ello **se recomienda:**

6. Promover el diálogo intersectorial sobre los beneficios y riesgos del uso de los datos relativos a salud, en clave de derechos, y fomentar consensos en relación a temas tales como propiedad, uso, cesión y transferencia de datos, donación, puesta en valor, prácticas éticas, bases de datos abiertas, uso de redes sociales en salud, la telemedicina y la formación técnico-profesional e individual, todo ello a efectos de fortalecer la construcción de una ciudadanía sanitaria.

7. Reconocer el desequilibrio estructural entre quienes producen la recolección, almacenamiento, tratamiento y uso de datos en salud y los usuarios del sistema sanitario, como la parte más vulnerable de la relación.

8. Colaborar en la disminución de la brecha digital y mejorar las habilidades tecnológicas para que no constituyan una barrera en el ejercicio de los derechos vinculados a los datos en salud.

9. Fortalecer una ciudadanía sanitaria con eje en la protección de datos personales referidos a salud, mediante procesos informados, participativos y transparentes que propicien y refuercen el conocimiento de los derechos y obligaciones involucrados en estos procesos.

III. GARANTÍAS.

La finalidad de las normas regulatorias en materia de datos es la protección de los derechos personalísimos en general y de la información personal en particular, mediante la cual se logran configurar perfiles tanto individual como social, profesional, sanitario o económico –entre otros-, para permitir se mantengan en la esfera de la intimidad y privacidad, rechazando en principio, toda posibilidad de utilización de datos personales por parte de terceros sin autorización de su titular.

A través del articulado de la Ley Nº 25.326 se establecen una serie de pautas protectorias y tutelas preventivas en materia de datos personales, que incluyen los datos sensibles y entre ellos los vinculados a la salud, en orden a su posibilidad de causar al titular algún daño o discriminación, cierta o potencial.

En función de lo expuesto y analizado el acto impacto que las innovaciones tecnológicas tienen en el sector sanitario, **se recomienda**:

10. Asegurar al titular del dato acceder a todo registro almacenado sobre su salud en algún repositorio sea público o privado y obtener una copia en un formato que le permita su posterior utilización y ejercicio de sus derechos.
11. Garantizar al titular, a su pedido, la cesión o transferencia de sus datos personales referidos a salud, de responsable a responsable de la atención sanitaria, a fin de compartir la información de sus registros médicos electrónicos, sin perjuicio del lugar de registro original, con las protecciones y medidas de seguridad adecuadas.
12. Asegurar al titular del dato el derecho a otorgar autorizaciones, preferencias y control del acceso, cesión y transferencias de la información sanitaria, exceptuando aquellas situaciones en que el acceso sea necesario para el normal desarrollo de las actividades de prestadores o financiadores sanitarios.
13. Requerir el consentimiento expreso del titular del dato en el supuesto de tratamiento incompatible con la finalidad de origen de la recolección, excepto en los casos en los que los datos recogidos puedan ser plenamente disociados y en consecuencia no puedan ser atribuidos a persona determinada o determinable.
14. Promover procesos de disociación de los datos personales de salud, a los fines de su tratamiento por el responsable cuando se considere adecuado, así como criterios para la implementación de técnicas de disociación.
15. Si es posible asegurar que el dato sanitario esté disociado no se considerará dato sensible y podrá ser utilizado para investigaciones científicas, estadísticas o actividades análogas, de conformidad con lo prescripto en la Ley Nº 25.326 y criterios éticos en la materia.

16. Ejercer una gobernanza efectiva de los conjuntos de datos que involucren a toda la población y en particular a los sectores más vulnerables, evitando cualquier estereotipo o patrón que pudiere generar exclusión, penalización, segmentación, estigmatización o discriminación de cualquier tipo –y especialmente sobre la salud- y que pueda derivar en daños individuales o colectivos.

IV. TRATAMIENTO DEL DATO EN SALUD

Como principio general, la Ley Nº 25.326 establece que ninguna persona puede estar obligada a proporcionar datos sensibles y que éstos solo pueden ser tratados 1) cuando medien razones de interés general autorizados por la ley; 2) se encuentren disociados o; 3) se preste el consentimiento informado (art. 7).

Respecto de los **datos de salud** la ley estableció que los establecimientos sanitarios públicos o privados, así como los profesionales vinculados a las ciencias de la salud, están autorizados a recolectar y tratar datos de los pacientes atendidos o que estén o hubieran estado bajo tratamiento de aquellos, respetando en todas las instancias el secreto profesional (art. 8) y sin necesidad de consentimiento (Opinión AAIP).

Por su parte, el responsable o usuario del archivo de datos personales está obligado a adoptar las medidas técnicas y organizativas necesarias para garantizar su seguridad y confidencialidad (Resolución Nº 47/2018 AAIP). En este sentido se debe evitar su adulteración, pérdida, consulta o tratamiento no autorizado y permitir detectar desviaciones de información, sean intencionales o no, provengan de la acción humana o técnica (art. 9).

Asimismo, la autorización para el tratamiento del dato es condición necesaria pero no suficiente ,por lo que se debe tenerse presente a este respecto el principio de información y de calidad del dato (art. 4).

La norma otorga la posibilidad de que los datos puedan ser tratados con finalidades estadísticas o científicas, siempre que sean disociados, ello es, asegurar la imposibilidad de identificar a su titular (ver Resolución 4/2019 AAPI).

En caso de modificarse la finalidad de la recolección o tratamiento del dato en salud por resultar incompatible con la de origen, para su tratamiento deberá solicitarse el consentimiento a su titular.

En suma, resultan aplicables a los datos relativos a la salud los principios generales en materia de protección de datos, a saber: deben ser pertinentes; recabados con una finalidad específica; no pueden ser utilizados para una finalidad distinta o incompatible con la que motivó su obtención; recogidos bajo el principio de legalidad, en forma licita y legal; inscriptos en registros habilitados (publicidad); bajo el control de organismos al efecto; con integridad y seguridad en su recolección, tratamiento y cesión a terceros.

Por ello **se recomienda**:

17. Implementar mecanismos de obligatoriedad de notificación al titular del dato y a la autoridad de aplicación de la Ley Nº 25.326, sin dilación indebida, de cualquier incidente de seguridad susceptible de causar un riesgo o daño significativo, cierto o potencial. La notificación deberá realizarse de manera enunciativa pero no limitativa, indicando los datos que puedan estimarse afectados, fecha, motivo del incidente, los hechos relacionados con este, efectos y medidas correctivas implementadas de forma inmediata y definitiva.

V. PROHIBICIÓN DE USO CON FINES DISCRIMINATORIOS.

Resulta innegable el potencial que poseen los datos en salud para contribuir a la mejora en el acceso, diagnóstico, tratamiento, equidad, calidad y gestión de la atención sanitaria, así como en actividades científicas y académicas para la generación de conocimiento.

Los datos tienen el poder de revolucionar la atención sanitaria, pero también el riesgo de provocar un desequilibrio de poder entre ciudadanos, gobiernos y empresas. Así, la consolidación de posiciones monopólicas podría afectar derechos fundamentales, intereses personales, la equidad y el acceso a la salud, traspasando incluso fronteras ante la carencia de regulaciones jurídicas y éticas, sólidas y comunes, para el tratamiento de los datos personales.

Por ello **se recomienda**:

18. Prohibir que los datos en salud puedan ser utilizados en la elaboración de perfiles o apreciación de conductas tendientes a discriminar a su titular por cualquier motivo.
19. Permitir al ciudadano el derecho a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos, incluida la elaboración de perfiles, que le produzca efectos jurídicos perniciosos o lo afecte de forma negativa, con las excepciones previstas por ley.

VI. DERECHO DE SUPRESIÓN EN EL AMBITO SANITARIO.

Se recomienda:

20. El responsable del tratamiento del dato podrá oponerse a la solicitud de rectificación o supresión de datos personales de salud efectuada por su titular, mediante simple decisión fundada, cuando dicho ejercicio pudiere afectar a su criterio intereses o derechos del titular del dato de salud, derechos propios, de terceros o el interés público.

VII. CESIÓN Y TRANSFERENCIA.

Se recomienda:

21. Propiciar que la cesión y transferencia de datos personales de salud sea lícita en caso de resultar necesaria para la prestación de un servicio sanitario, prevención, diagnóstico, tratamiento o gestión de servicios sanitarios, entre otras, estableciéndose que el receptor de esos datos personales tenga las mismas obligaciones que quien originó dicha transferencia (responsabilidad solidaria).

VIII. CAPACITACIÓN.

Se recomienda:

22. Promover programas de capacitación permanente para los integrantes del sector sanitario o afines, con competencia específica en la temática.
23. Concientizar en el uso responsable de los datos personales relativos a la salud al personal de empresas de servicios de datos, prestadores y financiadores del sector salud, como así también a los ciudadanos en general.

ANEXO I. NORMAS APLICABLES

- Constitución Nacional (art. 43 y ccdantes)

- Código Civil y Comercial de la Nación (art. 52 a 59 y ccdantes)
- Ley Nº 26.529
- Ley Nº 25.326, Resoluciones Nº 47/2018 y 4/2019 AAIP y Decisión Administrativa Nº 307/18
- Ley Nº 25.506
- Ley Nº 26.160
- Ley Nº 26.742
- Ley Nº 24.240
- Decreto Nº 415/2006
- Decreto Nº 1160/2010
- Código Penal (art. 153)
- Anteproyecto de Reforma del Código Penal
- Resolución Nº 189/2018 SGS (Estrategia Nacional de Salud Digital 2018-2024)

‘

Anexo II. INTEGRANTES DE LA MESA DE DIALOGO

- ☐ Alejandro López Osornio (Director Nacional de Sistemas de Información en Salud. Secretaría de Gobierno de Salud de la Nación)

☐ Daniel Rizzato Lede (Director de Desarrollo de Sistemas Informáticos. Secretaría de Gobierno de Salud de la Nación)

☐ Emiliano López (Coordinador Nacional de Telesalud. Secretaría de Gobierno de Salud de la Nación)

☐ Eduardo Bertoni (Director de la Agencia de Acceso a la Información Pública, AAIP)

☐ Eduardo Cimato (Director Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública)

☐ Roberto Moldes (Secretaría de Gobierno de Modernización de la Nación)

☐ Fernando Avellaneda (Interventor del Instituto de Previsión y Seguridad Social de la Provincia de Tucumán)

☐ Gustavo Caramelo (Juez Nacional en lo Civil)

☐ Silvia Monet (Gerente General ADECRA)

☐ Miguel Rosso (Presidente Colegio Médico Provincia de Buenos Aires Distrito V. CONFEMECO)

☐ Antonio Luna (Hospital de Pediatría SAMIC Prof. Dr. Juan P. Garrahan)

☐ Oscar Mando (CEMIC)

☐ Daniel Luna (Hospital Italiano)

☐ Fernando Plazzotta (Hospital Italiano)

☐ Juan Fuselli (Sociedad Argentina de Cardiología)

☐ Andrés Brandolini (Observatorio de Salud Facultad de Derecho UBA)

☐ Martín Testa (Observatorio de Salud Facultad de Derecho UBA)

☐ Laura Bilotta (Observatorio de Salud Facultad de Derecho UBA)

☐ Fiorella Bianchi (Observatorio de Salud Facultad de Derecho UBA)

☐ Eduardo Lombardi (Observatorio de Salud Facultad de Derecho UBA)

☐ Claudia Dreyer (médica)

☐ Guillermo Schot Landman (abogado)

☐ Santiago Troncar (Consultorio Móvil)