Preguntas y respuestas

1° Seminario Técnico: Ley 21.719 en centros de investigación clínica: del deber legal a la práctica metodológica y bioética

La Serena Research
COMITÉ ÉTICO CIENTÍFICO

1

¿Habría que hacer un ICF distinto?

La respuesta es que depende de si se cuenta con una base de licitud que habilite el tratamiento de datos, ya que para efectos del cumplimiento de la Ley N.° 21.719 y la Ley N.° 20.120, debemos distinguir con claridad entre dos ámbitos de tratamiento de datos dentro de nuestra institución:
1. Ámbito Asistencial e Institucional, cuando el Centro actúa como prestador, los datos personales que el centro recopila en las fichas clínicas para consultas, urgencias o exámenes se rigen por la Ley N°20.584 y la Ley N°19.628/21.719. Aquí la finalidad es médico-asistencial, el responsable legal es el Director del Centro y la información debe conservarse por 15 años por mandato de salud pública. Debiendo distinguir la base de licitud con la que se realiza el tratamiento y si es necesaria la obtención de un FCI.
2. Ámbito de Investigación Biomédica, en el contexto de ensayos clínicos, cuando el centro actúa como sitio de investigación para un protocolo farmacéutico, el tratamiento de los datos de los participantes se rige por la Ley N°20.120 y el Reglamento del DS N°114. En este sentido, los datos solo pueden tratarse bajo el consentimiento informado aprobado por el Comité de Ética Científica, debiendo mantenerse en seudonimización y los responsables de su conducción ante la ley son el Patrocinador y el Investigador Principal.
Por tanto, los datos asistenciales de la ficha clínica institucional no constituyen una base de datos propia libremente transferible al ensayo clínico, debiendo respetarse en todo momento el principio de finalidad, la base de licitud y las exigencias de visación ética previa que correspondan.



2

¿Que ocurrirá con las tesis de post grados? ya que los datos analizados permanecen en la Universidad o se publica por parte del ente académico.



Se debe considerar lo siguiente:

1. La Ley N.° 21.719 no opera con efecto retroactivo. Las tesis de postgrado finalizadas, aprobadas o cuyos datos se recolectaron legítimamente antes del 1 de diciembre de 2026 no sufren invalidez ni sanciones.
2. Por su parte las publicaciones académicas, los datos y resultados de tesis ya publicados o guardados en repositorios universitarios en forma anonimizada o seudonimizada están amparados por las excepciones de investigación científica de la ley (Art. 16 quinquies y Art. 16 bis).

El tratamiento continuo a futuro, si es realizado por la universidad, por medio de cruces o reutilizaciones de esas bases de datos personales identificables a contar de diciembre de 2026, deberán ajustarse a la nueva ley (aplicando anonimización o la base de licitud que corresponda).

¿El consentimiento de un titular puede considerarse un mecanismo adecuado para justificar la transferencia internacional de datos?

La respuesta es si, pero la Ley contempla estándares que deberán cumplirse para un adecuado tratamiento de datos. El Artículo 27 de la Ley N.º 19.628 (modificada por la Ley N.º 21.719) divide las operaciones de transferencia internacional de datos en dos niveles normativos:

1. Vías Ordinarias o Estructurales (Art. 27 inc. 1.º): Constituyen la regla general para flujos continuos o masivos de información, pudiendo realizarse al cumplir con lo siguiente:
   - Cuando los datos se transfieran a países u organizaciones que posean niveles adecuados de protección determinados por la Agencia de Protección de Datos Personales.
   - Cuando la transferencia quede amparada por cláusulas contractuales tipo, normas corporativas vinculantes u otros instrumentos jurídicos suscritos entre las partes que otorguen garantías equivalentes y derechos exigibles.
   - La existencia de modelos de certificación o cumplimiento aprobados por la autoridad.

Vía Excepcional / Regla de Descarte (Art. 27 inc. 2.º letra a): En ausencia de una decisión de adecuación o de las garantías contractuales indicadas, la ley dispone expresamente que se podrá realizar una transferencia cuando:

"**Exista consentimiento expreso del titular de datos para realizar una transferencia internacional de datos específica y determinada".**

Ahora bien, para que el consentimiento otorgado por el titular se considere un mecanismo legalmente adecuado frente a la autoridad de control, debe reunir las siguientes condiciones imperativas:
Debe como ya fue dicho, ser una manifestación de voluntad libre, específica, inequívoca, previa e informada, otorgada mediante una declaración escrita o por un medio tecnológico equivalente.
Se debe considerar que para que el consentimiento sea jurídicamente válido en transferencias internacionales, el responsable debe informar explícitamente al titular antes de la recolección:

1. La transferencia de sus datos a un tercer país u organización internacional.
2. Si dicho país cuenta o no con un nivel adecuado de protección.
3. En caso de no contar con ello, las salvaguardas o medidas de seguridad que se adoptarán para resguardar su información

Para el caso de protocolos de investigación clínica y Formularios de Consentimiento Informado sometidos a evaluación de Comités de Ética Científica, esta regulación implica la observancia de tres reglas a considerar:

1. El consentimiento otorgado por el participante en el FCI autoriza válidamente la salida de sus datos personales seudonimizados o codificados hacia el extranjero (por ejemplo, a laboratorios centrales o patrocinadores en EE. UU. o Europa), siempre que se haya especificado la finalidad, el país de destino y el uso de técnicas de encriptación y/o seudonimización.
2. Si la transferencia internacional incluye datos vinculados al envío de muestras biológicas para investigaciones futuras o biobancos opcionales, dicho consentimiento no puede condicionar la participación en el estudio principal, exigiendo una casilla de verificación independiente.
3. Aún cuando se cuente con el consentimiento del participante en el FCI, el patrocinador y el centro de investigación deben respaldar la relación institucional mediante un Acuerdo de Transferencia de Datos, garantizando la cobertura de seguridad que establece la Ley, evitando fundamentar flujos masivos continuos únicamente en la excepción del consentimiento individual.

¿Qué reglas de conservación y eliminación aplicarán a las distintas copias de un mismo dato? Pienso en ISF físico, eISF, ficha clínica, respaldo de correo, carpetas compartidas y sistemas del patrocinador: ¿cómo evitaremos tanto la eliminación prematura como la conservación indefinida?

Conforme a la ley 21.719, cada copia de un mismo dato es un tratamiento en sí misma. Esto vale para el ISF físico y el electrónico, la ficha clínica, un correo con un archivo adjunto, una carpeta compartida o el sistema del patrocinador. Por eso, cada copia necesita una finalidad, un responsable y un plazo de conservación definidos. Así se desprende de los principios de finalidad y proporcionalidad (art. 3º Ley 21.719). La regla general de la ley es que los datos se conservan solo mientras sean necesarios para la finalidad para la que se recogieron, y después se eliminan o anonimizan. La misma ley admite conservarlos por más tiempo cuando otra norma lo autoriza (ej. normativa sobre fichas clínicas de buenas prácticas clínicas sobre documentación esencial de los ensayos, que fijan plazos mínimos de conservación).

En la práctica, conviene distinguir dos tipos de copias. Las primeras son los registros oficiales: la ficha clínica, el ISF y los sistemas del patrocinador. Estos registros tienen una finalidad regulatoria propia y deben conservarse íntegros durante todo el plazo mínimo aplicable. Eliminarlos antes de tiempo puede ser tan problemático como guardarlos sin límite. Las segundas son las copias de trabajo o duplicadas: respaldos de correo, carpetas compartidas, descargas locales o impresiones. Normalmente estas copias no tienen una finalidad autónoma, porque su información ya está en un registro oficial. A ellas se aplica el criterio de minimización: solo deberían existir mientras se necesitan para una tarea concreta y deberían eliminarse apenas esa tarea termine. Sin embargo, puede haber matices. Por ejemplo, un correo puede ser el único respaldo de una comunicación relevante para el estudio. Por eso, la calificación de cada copia conviene hacerla caso a caso.

Para evitar tanto la eliminación prematura como la conservación indefinida, algunas medidas útiles son:

- Un inventario de copias por estudio, que indique dónde está cada una y quién la administra.
- Una tabla de plazos de conservación, que señale para cada tipo de registro la norma o el contrato que fija su plazo.
- La designación de una "copia maestra" para cada documento, de modo que las demás se traten como copias de trabajo.
- Procedimientos de eliminación o anonimización, con responsables definidos, y un registro o certificado que deje constancia de lo eliminado.
- Coordinación contractual con el patrocinador, para que el contrato regule el plazo de archivo, quién autoriza la destrucción y qué ocurre con los datos al cierre del estudio.

Lo central es poder explicar, frente a cualquier copia, por qué existe, quién la custodia y hasta cuándo debe conservarse. En concreto, y particularmente en el contexto de datos sensibles, se requiere una evaluación de impacto donde la pregunta "¿por que existe el dato?" debe responder por idoneidad, necesidad y proporcionalidad estricta (de entrada y de salida).

¿Cómo resolveremos una solicitud de supresión o bloqueo de datos de un participante sin alterar la trazabilidad, los datos fuente ni las obligaciones de archivo del ensayo? ¿Quién tomará y documentará esa decisión?

Para abordar la pregunta se debe considerar que regla general en investigación biomédica y protección de datos es que la revocación del consentimiento o la solicitud de supresión NO opera necesariamente de manera retroactiva sobre los datos clínicos obtenidos con anterioridad a la fecha del retiro.

Se contempla una excepción legal expresa a la supresión en el artículo 7º inciso 2º de la Ley Nº21.719. La Ley de Protección de Datos Personales contempla excepciones en las que no procede la eliminación de los datos, específicamente cuando el tratamiento sea necesario:

- Para el cumplimiento de una obligación legal.
- Por razones de interés público en el área de la salud pública.
- Para tratamientos con fines científicos o de investigación que atiendan fines de interés público.

A su vez las normas de farmacovigilancia contemplan un deber de cuidado y de integridad de las fichas clínicas como documentos fuente (fichas clínicas del centro de salud, exámenes de laboratorio, constancias de dosis), entendiéndose que son registros médicos regulados por la Ley Nº20.584 y la Resolución Exenta Nº5.174 del ISP, por lo que se entiende que no se pueden alterar, borrar o destruir los datos fuente históricos, ya que hacerlo constituye una infracción gravísima a la trazabilidad, al deber de archivo obligatorio y a las normas de farmacovigilancia. De todas formas, hay que esperar lo que dictamine el reglamento de la Ley Nº19.628 (modificada) y el inicio del Servicio de la Agencia de Protección de datos para tener mayor claridad.

Lo que queda más claro es que frente a la solicitud del participante, se debe contemplar necesariamente lo siguiente:

1. Cese Inmediato de Recolección Futura a contar del momento de la revocación, interrumpiéndose de inmediato cualquier procedimiento, visita, llamada de seguimiento o captura de nuevos datos clínicos.
2. Bloqueo de la Ficha Clínica en la base de datos del estudio, el sujeto es marcado con el estado revocación del consentimiento, por lo que se debe congelar o bloquea su registro para evitar ingresos o ediciones posteriores, cumpliendo la función de bloqueo del Artículo 8ºter de la Ley Nº21.719.
3. Y respecto de las muestras biológicas sobrantes, si el participante además exige la eliminación de sus muestras biológicas almacenadas por ejemplo, en biobancos o estudios futuros opcionales, las muestras no consumidas deben ser destruidas o devueltas de conformidad con el Artículo 6º del DS N.º 114 y la Res. Ex. N.º 5.161 del ISP, emitiéndose un Certificado de Destrucción.

Finalmente, respecto de quien debe actuar y tomar las medidas que resulten pertinentes, se debe distinguir:

El Investigador Principal debe recibir la solicitud del participante (o de su representante legal), detiene de inmediato las intervenciones del estudio y registra la decisión en la Ficha Clínica del paciente, debiendo consignar la fecha, hora, motivo declarado si lo hubiere y dejar constancia de que se le explicó al participante respecto del cese de la recolección de datos en el futuro, pero que la información obtenida hasta la fecha se mantendrá seudonimizada en los archivos del ensayo por exigencia legal y de seguridad.
Por su parte los patrocinadores o encargados de protección de datos deben analizar el alcance de la solicitud y emitir la respuesta formal por escrito dirigida al participante o tramitada a través del centro en un plazo no mayor a 30 días. El contenido de la respuesta debe confirmar la interrupción de la recolección de datos, informa la destrucción de muestras sobrantes adjuntando el certificado si aplica, y explica fundadamente que los datos históricos recopilados previamente permanecen archivados bajo código de seudonimización.

Preguntas y respuestas

1° Seminario Técnico: Ley 21.719 en centros de investigación clínica: del deber legal a la práctica metodológica y bioética

La Serena Research
COMITÉ ÉTICO CIENTÍFICO

6

¿Esta ley será retroactiva? ¿Los comités de ética estarán al tanto para aprobar/modificar los consentimientos de nuevos estudios a futuro, para que cumplan con esta normativa?, o esa responsabilidad recaerá en los sites?

La fecha de entrada en vigencia general de la Ley N°21.719 hasta hoy es el 1 de diciembre de 2026, y como toda norma, por regla general se rige por el principio de irretroactividad, por lo que puede entenderse que la ley no tiene efecto retroactivo sancionatorio. Esto significa que no se puede sancionar o invalidar la recolección de datos realizada legítimamente antes del 1 de diciembre de 2026 bajo el alero de la antigua Ley N°19.628. No obstante, las exigencias de aplicación de la ley modificada sobre el tratamiento continuado de datos personales, aunque la recolección previa haya sido válida, debe realizarse conforme a la nueva normativa. Por lo tanto, a contar del 1 de diciembre de 2026, todo tratamiento activo de datos que continúe ejecutándose deberá ajustarse a la nueva Ley N°21.719, y los participantes podrán ejercer los nuevos derechos ARCOP (Acceso, Rectificación, Supresión, Oposición, Portabilidad y Bloqueo) sobre sus datos almacenados.



En cuanto a quién es responsable de adaptar los consentimientos y cumplir la nueva normativa, se debe considerar la estructura de gobernanza de datos, recayendo la carga principal en el responsable del tratamiento, que comúnmente es el patrocinador.

7

¿Cuando hayan auditoria, se darán cuanta si no se cumple la ley? ¿Quién supervisa?



En cuanto a Datos Personales, La Agencia de Protección de Datos Personales creada por la Ley N°21.719, será la autoridad autónoma de derecho público encargada de fiscalizar el cumplimiento de los principios, derechos ARCOP, medidas de seguridad y transferencias internacionales de datos personales en todo el territorio nacional, contando con potestad sancionadora directa.

Es importante considerar que los procesos de auditoría permitirán a la autoridad establecer el cumplimiento de la nueva normativa, ya que por medio de la verificación e inspección de los FCI por ejemplo, se determinará si se ha dado consentimiento expreso del titular de datos para realizar una transferencia internacional de datos específica y determinada, si se ha dado la información necesaria, etc.

La Ley exigirá a toda persona natural o jurídica justificar ante la Agencia, que realiza un adecuado tratamiento de datos, no basta la sola declaración, por lo que es necesario realizar los procesos de adecuación que sean pertinentes, evitando incumplimientos que puedan derivar en multas o sanciones.

Preguntas y respuestas

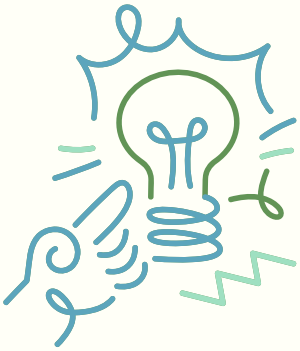
1° Seminario Técnico: Ley 21.719 en centros de investigación clínica: del deber legal a la práctica metodológica y bioética

La Serena Research
COMITÉ ÉTICO CIENTÍFICO

8

¿Solicitar la fotocopia del carnet identidad de los pacientes a su ingreso sería errado ?

La solicitud que se indica puede constituir una infracción al Principio de Proporcionalidad y Minimización de Datos, ya que bajo el Artículo 3º letra c) de la Ley N°21.719, todo tratamiento de datos debe limitarse estrictamente a aquéllos que resulten necesarios, adecuados y pertinentes en relación con los fines del tratamiento. Para verificar la identidad de una persona al momento de su enrolamiento o atención, el fin legítimo se cumple mediante la comprobación o exhibición visual presencial de la cédula por parte del profesional o Ministro de Fe por lo que retener una fotocopia constituye una captura excesiva e innecesaria de datos.



Para cumplir con la legislación de protección de datos, los centros de investigación deberían sustituir la práctica de fotocopiados por constataciones visuales que pueden ser realizadas por el profesional que realiza la toma de consentimiento, solicitando la cédula de identidad al participante, dejando una constancia en la ficha clínica o en el formulario de consentimiento informado, por medio de una glosa que de cuenta de la verificación.

9

En un reporte de SAE ¿Nombrar el nombre del hospital estaría mal ?



Incluir el nombre del hospital en un SAE, no implica necesariamente una infracción a la ley. El problema podría aparecer cuando el nombre del hospital se combina con otros datos del reporte. La ley considera que una persona es identificable cuando se puede saber quién es, aunque sea de forma indirecta. Si el reporte incluye, por ejemplo, el hospital, la edad, el sexo, la fecha de hospitalización, puede bastar para saber de quién se trata. En esos casos, lo que importa no es el nombre del hospital por sí solo, sino lo que el reporte completo permite deducir.

En la práctica, la regla es incluir en el reporte solo lo indispensable. Se puede identificar el centro y usar el código del participante, pero no es necesario agregar otros datos que puedan permitir su identificación (ej. número de ficha clínica u hospital). Conviene preguntarse si cada dato adicional es realmente necesario. Como el riesgo de identificar al participante depende de cada caso, no hay una regla única que sirva para todos los reportes, sino que debe analizarse caso a caso.

¿Qué controles concretos debemos exigir a los vendors que manejan datos del estudio? ¿Bastará el contrato actual o necesitaremos revisar instrucciones de tratamiento, accesos, subcontratación, incidentes y devolución o eliminación de datos?

Un contrato que solo tenga una cláusula genérica de confidencialidad no cumple con el estándar de la Ley Nº 21.719. El artículo 15 bis exige que la relación entre el responsable y el proveedor que trata datos por su cuenta (encargado) se rija por un contrato con un contenido mínimo. Por eso corresponde establecer, al menos, los siguientes controles:

A. Controles que exige directamente la ley

- Contenido mínimo del contrato: objeto del encargo, duración, finalidad del tratamiento, tipo de datos, categorías de titulares y derechos y obligaciones de las partes (art. 15 bis).
- Instrucciones de tratamiento: el proveedor debe tratar los datos solo según las instrucciones del responsable. No puede usarlos para otro fin ni cederlos. Si lo hace, responde personalmente por las infracciones y solidariamente con el responsable por los daños (art. 15 bis).
- Subcontratación: solo con autorización específica y por escrito del responsable. Si el proveedor delega, sigue siendo solidariamente responsable (art. 15 bis).
- Devolución o eliminación: al terminar el encargo, el proveedor debe eliminar los datos o devolverlos al responsable (art. 15 bis).
- Confidencialidad: quienes accedan a los datos quedan sujetos al deber de secreto (art. 14 bis).

B. Controles que derivan de las obligaciones del responsable

La ley pone sobre el responsable la carga de adoptar medidas de seguridad y de poder acreditarlas, y de reportar a la Agencia los incidentes de seguridad. Como esos datos los maneja el proveedor, el responsable solo puede cumplir esas obligaciones si el contrato le exige al proveedor lo siguiente:

- Accesos: acceso restringido al personal autorizado, con registro de quién accede, cuándo y a qué datos.
- Medidas de seguridad: obligación de mantener medidas técnicas y organizativas proporcionales al riesgo, especialmente porque son datos de salud y genéticos.
- Incidentes: obligación de avisar al responsable de cualquier incidente de seguridad dentro de un plazo y con un contenido definidos, y de colaborar en la respuesta. La ley no fija ese plazo; lo define el contrato.
- Evidencia de cumplimiento: derecho del responsable a pedir información, certificaciones o auditorías que le permitan acreditar el cumplimiento ante la Agencia.
- Certificación de término: constancia escrita de que los datos se eliminaron o devolvieron, incluidos los que tengan los subcontratistas.

C. Si los datos salen del país

- Transferencia internacional: el contrato debe indicar dónde se alojan los datos y tener una base de licitud conforme a los artículos 27 y 28. Mientras la Agencia no apruebe sus propias cláusulas, existen las cláusulas modelo aprobadas por la Resolución Exenta RAEX202503748, con un modelo para la relación entre responsables y otro para la relación entre responsable y encargado.

Estas respuestas tienen carácter general e informativo, y se entregan solo para apoyar la reflexión de los participantes del webinar. No constituye asesoría legal ni reemplaza el análisis de cada caso, que debe hacer cada institución con sus propios asesores. El Comité Ético Científico que la proporciona no asume responsabilidad por las decisiones que se tomen o los efectos que se produzcan a partir de su contenido.

Para mayor orientación y/o consultas:

victor.abarca@iclsr.cl
oscar.caceres@iclsr.cl
nicolas.palacios@iclsr.cl

La Serena Research
COMITÉ ÉTICO CIENTÍFICO