UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
ESCUELA DE GRADUADOS

PROGRAMA DE MAGISTER EN DERECHO,

CON Y SIN MENCIÓN

ACTIVIDAD DE FORMACIÓN EQUIVALENTE A TESIS

"INTEROPERABILIDAD DE LAS FICHAS CLÍNICAS"

Alumno: José Miguel Catepillán Friederichs
Profesora guía: Lorena Donoso Abarca

29 de diciembre de 2021
Santiago, Chile

AGRADECIMIENTOS

A mi familia, especialmente, a mi padre Siegfried por su cariño e incondicional apoyo,

A mi madre Carolina por su amor y su resiliente trayectoria como referencia,

A mi abuelo Jorge por ser un imprescindible a nivel personal e intelectual.

A Josefa por su inagotable cariño, paciencia y apoyo,

A Lorena Donoso por su generosidad con los conocimientos y perspicaz orientación,

A la Konrad Adenauer Stiftung por confiar en mí durante este camino.

RESUMEN Y PLANTEAMIENTO DEL PROBLEMA.

La regulación de la ficha clínica se encuentra en el Código Sanitario, la ley 20.584 y el Decreto N41, de 2012, que aprueba el reglamento sobre fichas clínicas.

Si bien la constitución garantiza a todas las personas la promoción, protección y recuperación de la salud, y las normas sectoriales desarrollan de qué manera se dará cumplimiento a este derecho, incluyendo el acceso a la información de salud por los profesionales que participen directamente de la atención del paciente, la normativa no se hace cargo de normar como se asegurará la disponibilidad de la información, especialmente en relación a cómo se accederá a la información que consta en fichas clínicas almacenadas en sistemas de distintos prestadores de salud. Esto ha impactado negativamente en la manera en que se gestiona e interactúa la información clínica con el propósito de que esté disponible cuándo y dónde se le necesita, generando efectos indeseados para todos los actores del proceso asistencial, principalmente, pacientes, prestadores (públicos o privados) y del Estado.

Como consecuencia adicional, los prestadores ven dificultada su labor en la relación de acciones y prestaciones de salud, al no contar con la información necesaria para garantizar la continuidad del cuidado del paciente. El sistema integrado de salud es más ineficiente, al tener que repetir exámenes de laboratorio e imágenes que ya constan en sistemas de otros prestadores y se generan, además, riesgos a la salud de las personas, al no ser factible que el prestador verifique si los fármacos que prescribe tienen riesgo de efectos adversos por interacciones con otros fármacos o condiciones preexistentes del paciente.

Todo lo anterior es un efecto directo que de la información precisa se encuentre disgregada en los sistemas de distintos prestadores de salud, en formatos no consultables en línea o no reutilizables.

Si bien, conforme lo ha previsto la ley N° 20.584 y el Decreto N° 41, tanto el Estado como el sector privado han invertido ingentes recursos en el desarrollo de las fichas clínicas electrónicas, aún existen fichas en soporte papel. Esto agrega un desafío adicional, consistente en la digitalización de la información que consta en estas fichas, frente al riesgo de pérdida o destrucción.

Paralelamente, el Estado pierde la oportunidad de sistematizar la información de salud de la población impidiendo que el desarrollo de las políticas públicas de salud esté

acompañado de mayor evidencia. Como corolario, no posee las herramientas jurídicas y técnicas para responder a su mandato constitucional en materia de salud de un modo acorde a los criterios de eficiencia y eficacia. En este sentido, difícilmente podría el MINSAL “coordinar y ejecutar” las acciones de salud si no posee información precisa en el momento oportuno.

Como solución proponemos regular de manera específica las condiciones de acceso a la información, con independencia del prestador en el cual se haya generado y se almacene. A ello nos referiremos como interoperabilidad de la información clínica, que supone a su vez la interoperabilidad e los sistemas en los cuales consta. Con ello se busca que la información no sólo sea accesible, sino además trazable, y reutilizable. Ello permitiría que estas condiciones no dependan de la interpretación normativa, que resta certeza jurídica en una materia que es crítica desde el punto de vista de la concreción del derecho fundamental a la salud de las personas.

En el desarrollo de este trabajo explicaremos como hemos llegado a estas recomendaciones.

ÍNDICE

TABLA DE ACRÓNIMOS

APDP	Agencia de Protección de Datos Personales
API	Interfaz de programación de aplicaciones
ARCO	Derechos de acceso, rectificación, cancelación y oposición
ARCOP	Derechos de acceso, rectificación, cancelación, oposición y portabilidad
BID	Banco Interamericano de Desarrollo
CCD	Continuity of Care Document
CDA	Clinical Document Architecture
CDA Release 2	Clinical Document Architecture Version 2
CDH	Consejo de Derechos Humanos de la ONU
CE	Comisión Europea
CENS	Centro Nacional de Sistemas de Información en Salud
CEPAL	Comisión Económica para América Latina y el Caribe de la ONU
CESFAM	Centro de Salud Familiar
CGR	Contraloría General de la República
CMBD	Conjunto Mínimo Básico de Datos
CMF	Comisión para el Mercado Financiero
CMI	Cuenta médica interoperable
CPLT	Consejo para la Transparencia
CRUD	Create, Read, Update and Delete
DICOM	Digital Imaging and Communications in Medicine
DPS	Datos personales de salud
EIF	Marco Europeo de Interoperabilidad
EPIVIGILA	Sistema de Vigilancia Epidemiológica
ETSI	European Telecommunications Standards Institute
FCE	Ficha Clínica Electrónica
FCEI	Ficha Clínica Electrónica Interoperable
FHIR	Fast Healthcare Interoperability Resources
FINTECH	Financial Technology
FONASA	Fondo Nacional de Salud
FOS	Fuerzas de Orden y Seguridad Pública
GDPR	Reglamento General de Protección de Datos de la Unión Europea
HCR	Historia Clínica Resumida
HIMSS	Healthcare Information and Management Systems Society
HIS	Sistema de Información Hospitalario
HL7	Health Level 7
HL7 CCOW	Health Level 7 Clinical Context Object Workgroup
HL7 EHR	Health Level 7 Electronic Health Record
HL7 FHIR	Health Level 7 Fast Healthcare Interoperability Resources
HL7 V2	Health Level 7 Versión 2
HL7 V3	Health Level 7 Versión 3
HRP	Historia Resumen Paciente
HTTP	Hypertext Transfer Protocol
ICD-11	International Classification of Disease
IDA	Interchange of Data between Administration EU
IDIS	Instituto para el Desarrollo e Integración de la Sanidad
IEEE	Institute of Electrical and Electronics Engineers
IHE	Integrating Healthcare Enterprise
INDH	Instituto Nacional de Derechos Humanos
INE	Instituto Nacional de Estadísticas
INN	Instituto Nacional de Normalización
IP	Internet Protocol
IPS	International Patient Summary
ISAPRE	Instituciones de Salud Previsional
ISO	International Organization for Standardization
ISP	Instituto de Salud Pública
JSON	JavaScript Object Notation
LDDP	Ley Nº 20.584 sobre derechos y deberes de los pacientes
LOCBGAE	Ley Orgánica Constitucional de Bases Generales de la Administración del Estado
LOINC	Logical Observation Identifiers Names and Codes
LPVP	Ley Nº 19.628 sobre protección de la vida privada

MINECON	Ministerio Economía, Fomento y Turismo
NNA	Niños, niñas y adolescentes
NT	Norma técnica
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OID	Identificador Único de Objetos
OMS	Organización Mundial de la Salud
ONU	Naciones Unidas
OPS	Organización Panamericana de la Salud
PACS	Picture Archiving and Communication System
PAHO	Organización Panamericana de la Salud
PCR	Examen para la detección de COVID-19
PDLPDP	Proyecto de ley que “Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales” (boletín 11.144-07)
PDP	Protección datos personales
RACSEL	Red Americana de Cooperación sobre Salud Electrónica
RESTful API	Transferencia de Estado Representacional
SEGRES	Secretaría General de la Presidencia
SEREMI	Secretaría Regional Ministerial
SERNAC	Servicio Nacional del Consumidor
SIDRA	Sistemas Información de Red Asistencial
SNOMED CT	Systematized Nomenclature of Medicine Clinical Terms
SOA	Arquitectura Orientada a Servicios
SUPERSALUD	Superintendencia de Salud
SUSESO	Superintendencia de Seguridad Social
TC	Tribunal Constitucional
TCP	Transmission Control Protocol
TIC	Tecnologías de la información
TJUE	Tribunal de Justicia de la UE
UE	Unión Europea
XML	eXtensible Markup Language

INTRODUCCIÓN.

La salud corresponde a uno de los ámbitos de la vida del ser humano donde mayor incidencia ha tenido la innovación tecnológica a la hora de ampliar los horizontes de bienestar de toda la población. Este fenómeno queda claramente graficado al analizar la evolución que ha experimentado la ficha clínica con el paso del tiempo, puesto que gracias al avance tecnológico ha sido posible el paulatino reemplazo del papel por los medios digitales, los cuales favorecen una mayor versatilidad en su gestión.

Sin embargo, por consideraciones de índole culturales, legales, administrativas, operativas, económicas y tecnológicas, en Chile aún no es posible sostener que los frutos del progreso científico hayan permeado suficientemente a la salud y, en ello puede tener que ver los escasos avances en la interoperabilidad de la ficha clínica.

Puntualmente, nuestro sistema de salud se integra de un conjunto de prestadores individuales e institucionales con distintos niveles de especialización y alcance territorial, todos los cuales están obligados a elaborar y mantener fichas clínicas de los pacientes a los que atienden. Dicha obligación necesariamente se traduce en la generación constante de una cuantiosa cantidad de información de salud que, estando distribuida de manera inorgánica, resulta muy difícil de gestionar, tanto en el aseguramiento de la salud del paciente como en la elaboración y gestión de políticas públicas.

Nuestra investigación se ha centrado en la identificación de los efectos en los derechos del paciente y la identificación de las brechas normativas asociadas a la interoperabilidad de las fichas clínicas.

A partir del diagnóstico, nuestro objetivo general ha sido elaborar recomendaciones de modificaciones legales o reglamentarias, a la luz de la experiencia comparada y atendiendo a las exigencias que emanan de los actuales estándares de derecho de acceso a las acciones y prestaciones de la salud, de protección de datos personales y de ciberseguridad.

Luego, consideramos factible la generación de condiciones optimizadoras de los sistemas de información de salud en términos de eficiencia y eficacia, favoreciendo un mejor rendimiento del proceso asistencial en su integridad por la coordinación de cada uno de sus actores. Asimismo, su implementación permitiría facilitar el rol garante del Estado tanto respecto de la protección, promoción y recuperación de la salud como de la protección de

datos personales, asegurando a los pacientes un control real respecto de la información contenida en la ficha clínica.

En este orden de ideas, los objetivos específicos que guiaron la investigación fueron los siguientes:

- En primer lugar, recopilamos y sintetizamos la normativa sanitaria de las fichas clínicas con el propósito de determinar el estado de situación.
- Luego, nos planteamos el desafío de analizar qué se entiende por interoperabilidad de las fichas clínicas.
- En tercer lugar, investigamos las políticas públicas que se han intentado en materia de interoperabilidad de las fichas y la normativa en que se han basado, tratando de identificar las razones que explican que no haya prosperado su desarrollo.
- En cuarto lugar, identificamos y sintetizamos los estándares técnicos y normativos de interoperabilidad en las fichas clínicas basándonos en la experiencia de Australia, Canadá, España y Uruguay.
- Finalmente, analizamos la situación de Chile a la luz de los estándares de PDP de las fichas clínicas contemplados por las mencionadas cuatro jurisdicciones.

En nuestras conclusiones formulamos recomendaciones de política pública con el propósito de subsanar las brechas normativas necesarias para implementar la interoperabilidad en las fichas clínicas optimizando el rol del Estado en términos de eficiencia y eficacia, y con pleno respeto a los derechos de los pacientes.

Esperamos que lo anterior siente las bases de un proyecto de ley o norma reglamentaria que establezca claramente la obligación de la interoperabilidad de las fichas clínicas, el desarrollo de una política nacional de interoperabilidad, la adopción de mecanismos para cuantificar la madurez en este ámbito y la necesidad de uniformar y actualizar los estándares aplicables.

Asimismo, elaboramos una propuesta para implementar la interoperabilidad según las mejores prácticas existentes a nivel comparado, lo cual implica realizar modificaciones a la legislación e institucionalidad de PDP y de ciberseguridad, así como a la manera en que se debe llevar a cabo la transformación digital del sector salud.

El método de la investigación empleado fue el método tradicional de la dogmática jurídica, en combinación con el de análisis de derecho comparado y los propios del análisis de soluciones técnicas en su aplicación a problemas de política pública.

En el análisis de fuentes directas e indirectas se empleó la técnica de investigación documental bibliográfica (fichaje).

CAPÍTULO I. MARCO JURÍDICO DE LAS FICHAS CLÍNICAS.

1.- LAS GARANTÍAS FUNDAMENTALES DE PROTECCIÓN DE LA SALUD Y PROTECCIÓN DE DATOS PERSONALES COMO BASE DE LA INVESTIGACIÓN.

Iniciaremos la presentación de los resultados de nuestra investigación con el análisis de las normas constitucionales vigentes, en relación con la salud y la protección de datos personales, pues sobre esta base deberemos luego desarrollar nuestra propuesta.

Nos referimos al Capítulo III, sobre Derechos y Deberes Constitucionales y, más precisamente, en el artículo 19 Nºs 9º y 4º.

En efecto, el numeral 9º aborda la salud a partir de una delimitación en el accionar del Estado, según los siguientes términos:

> "9º.- El derecho a la protección de la salud.
> El Estado protege el libre e igualitario acceso a las acciones de promoción, protección y recuperación de la salud y de rehabilitación del individuo.
> Le corresponderá, asimismo, la coordinación y control de las acciones relacionadas con la salud.
> Es deber preferente del Estado garantizar la ejecución de las acciones de salud, sea que se presten a través de instituciones públicas o privadas, en la forma y condiciones que determine la ley, la que podrá establecer cotizaciones obligatorias.
> Cada persona tendrá el derecho a elegir el sistema de salud al que desee acogerse, sea éste estatal o privado;"

Es necesario considerar que el derecho a la protección de la salud, "en cuanto derecho social, se halla intrínsecamente ligado a otros atributos esenciales de la persona asegurados por la Constitución, v. gr., el derecho a la vida y a la integridad física y psíquica, como asimismo al derecho a la seguridad social, todos los cuales deben ser tutelados y promovidos para infundir legitimidad al ordenamiento".[1]

Por consiguiente, la misión del Estado, en relación con la protección de la salud de toda persona, consiste, en primer lugar, en proteger el libre e igualitario acceso a las acciones de promoción, protección y recuperación de la salud y rehabilitación de la persona, desde la etapa de gestación y hasta la etapa de cuidados y acompañamiento en el momento de

[1] STC Rol Nº 976-2007, considerando 32. En esta misma línea, STC Nº 1.287-2008, considerando 32.

la muerte. Para este acceso igualitario es indispensable que el médico tratante pueda tener acceso a la información del paciente.

En segundo lugar, el Estado debe coordinar y controlar las acciones de salud. En consecuencia, el Estado debe procurar la existencia de un marco normativo que permita el acceso a esta información.

En tercer lugar, está obligado a garantizar la ejecución de las acciones de salud, ya sea que se presten a través de instituciones públicas o privadas, pero correspondiéndole de modo preferente al Estado, en desmedro de los privados.[2] Finalmente, al Estado le corresponde velar por el derecho de las personas a elegir el sistema de salud que estimen conveniente.

En estas dos últimas materias, es importante considerar que una persona podrá ser atendida por múltiples prestadores públicos o privados, o en distintos niveles de atención, esto es, primaria, secundaria o terciaria, por lo que el desafío de la interoperabilidad de la información es nacional y no puede depender de la voluntad de cada uno de los prestadores.

Como podemos apreciar, todos estos mandatos constitucionales son amplios y trascendentales para definir y precisar los deberes del Estado en relación con la regulación e implementación de la ficha clínica y su interoperabilidad.

A su vez, el numeral 4º consagra la protección de los datos personales bajo la siguiente técnica legislativa:

> "El respeto y protección a la vida privada y a la honra de la persona y su familia, **y asimismo, la protección de sus datos personales. El tratamiento y protección**

[2] De acuerdo con la Dirección de Estudios del TC, el deber preferente del Estado en materia de salud se caracteriza, en primer lugar, por tratarse de un "deber del Estado" y, por tanto, la conducta estatal respectiva se describe abstracta y genéricamente; es impuesta en interés general o de la colectividad; y no tiene correlato en derechos subjetivos. En segundo lugar, se trata de un deber "preferente" del Estado, lo que significa que el rol de este en dicha materia es principal, mientras que el de los privados es subsidiario. En tercer lugar, la Constitución utiliza la expresión "garantizar", es decir, busca dar certeza al titular del derecho de que las prestaciones efectivamente se llevarán a la práctica. Finalmente, este deber preferente del Estado se materializa "en la forma y condiciones que determine la ley". (STC 1.572 c. 22 y, en el mismo sentido, STC 1.589 c. 20, STC 1.629 c. 20, STC 1.636 c. 20, STC 1.710 cc. 121 y 122, STC 1.745 c. 21, STC 1.765 c. 20, STC 1.766 c. 20, STC 1.769 c. 20, STC 1.784 c. 22, STC 1.785 c. 20, STC 1.806 c. 22, STC 1.807 c. 20).

de estos datos se efectuará en la forma y condiciones que determine la ley;" (el destacado es nuestro).

En lo que toca a nuestra investigación, la relevancia de este numeral está dada por los contenidos que están incluidos en la ficha clínica, que no son otros que DPS, es decir, la información personal de individuos determinados o determinables en su esfera de salud, lo que posibilita que haya tantas fichas que contengan DPS como personas (titulares) existan.

Con todo, las prerrogativas de esta garantía fundamental no resultan sustantivas, sino más bien escuetas o limitadas, ya que el texto constitucional ha optado por delegar a una ley la regulación detallada de las formas y condiciones del tratamiento y protección de estos datos personales, a diferencia de otros países tanto de América Latina y del resto del mundo. Siendo así, nuestra Carta Magna nada consagra acerca de los derechos básicos de los titulares (ARCOP) o sobre la acción de *habeas data* que permite cautelar de modo expedito y eficaz su plena vigencia[3], con importantes riesgos desde el punto de vista de los derechos, por cuanto una interpretación estricta del texto vigente podría tornar tácitamente inconstitucionales a todos los instrumentos infra legales que pretendan desarrollar los contenidos de la garantía fundamental. Esto en base a lo que se dispone en los artículos 19 Nº 26 —referido a las normas que regulan o complementan garantías— y 63 Nº 2, -reserva legal-, en el texto vigente.

Siguiendo nuestro análisis, estimamos que para garantizar la continuidad del cuidado de la salud de las personas —en los términos que mandata la Constitución— es necesario que los profesionales que participan directamente en las acciones y prestaciones de salud de cada persona, tengan a su disposición, a lo menos, de los datos personales fidedignos sobre los diagnósticos previos, resultados de exámenes y tratamientos en curso, con

[3] Por ejemplo, en Sudamérica con algunos matices en la técnica jurídico-constitucional, las Constituciones de Argentina (artículo 43), Brasil (artículo 5º literal LXXII), Bolivia (artículos 130 y 132), Colombia (artículo 15) y Ecuador (artículos 66 literal 19 y 92), Perú (artículos 2º literal 6º y 200 literal 3º) consagran disposiciones relativas al *habeas data* y derechos ARCO. En Uruguay, si bien no está declarado en el texto constitucional, la ley de datos personales (Nº 18.331 de 2008) reconoce a esta materia como un derecho humano de conformidad al artículo 72, que explícitamente indica que la enumeración de derechos, deberes y garantías no posee un carácter taxativo.
Además, entre los países de la OCDE destacan Eslovenia (artículo 38), Hungría (artículo VI.2 del título referente a la Libertad y Responsabilidad), México (artículos 6º, 16, 20, y 28), Polonia (artículo 51), Portugal (artículo 35), Países Bajos (articulo 10) y Turquía (artículo 20).

independencia de que esa información conste en los sistemas informáticos del prestador que las realiza o de otros prestadores, para lo cual es esencial que los sistemas interoperen.

Adicionalmente, debemos tener presente que el 25 octubre 2021 fue publicada la ley Nº 21.383, que reformó el artículo 19 Nº 1 del texto constitucional, referente al derecho a la vida y a la integridad física y psíquica de la persona, agregando un inciso final nuevo que, en lo medular, consagra que "el desarrollo científico y tecnológico estará al servicio de la persona humana", sin perjuicio de que el proyecto de ley inicial buscaba consagrar la protección de los neuroderechos.

Si bien esta modificación es significativa para nuestra investigación, dado lo reciente de su incorporación, sería prematuro realizar un análisis detallado acerca de sus potenciales efectos.

En segundo lugar, corresponde al deber de coordinación del Estado, particularmente en relación con su responsabilidad de supervigilar las acciones relacionadas con la salud —según obliga el art. 19 Nº 9º inciso segundo de la Carta Fundamental—. Esta norma debe interpretarse en concordancia con el principio de legalidad consagrado en el artículo 7º, que demarca los contornos de la supremacía constitucional al establecer que los órganos del Estado actúan válidamente en la medida en que estén dotados de investidura regular, respeten el ámbito de sus competencias y lo hagan en la forma en que prescriba la ley. En consonancia con lo anterior, esta disposición constitucional prohíbe, respecto de toda magistratura, persona o grupo de personas, la atribución —ni siquiera en circunstancias extraordinarias— de otra autoridad o derechos que los que expresamente se les haya conferido en virtud de la Constitución o las leyes. Como sanción, el artículo 7º prescribe que todo acto en contravención a esta disposición es nulo y originará las responsabilidades y sanciones que la ley señale.

A ello debemos sumar que la fuerza normativa de estas disposiciones, así como de todo el texto constitucional, está dado por la consagración explícita de la supremacía constitucional en el artículo 6º, cuyo inciso segundo —para los efectos que aquí interesan— determina la obligatoriedad de todos y cada uno de los preceptos constitucionales respecto de toda persona, institución o grupo. En otras palabras, la Constitución, como norma jurídica, es vinculante y obligatoria respecto de sus destinatarios por medio de su eficacia directa y, para el caso de que se verifique una contravención, tendrán lugar las responsabilidades y sanciones que determine la ley —en voz del inciso final de la precitada norma—.

Estas normas resultan trascendentales para los efectos de esta investigación, por cuanto de su interpretación sistémica se puede desprender la existencia de la obligación jurídica de interoperabilidad de las fichas clínicas y el consiguiente deber del Estado de garantizarla, en el marco del deber de coordinación y control de las acciones de salud (Art. 19 Nº 9º) como, asimismo, de la protección de los datos personales (Art. 19 Nº 4º) en concordancia con los demás artículos antes citados.

2.- NORMAS LEGALES Y JURISPRUDENCIA RELEVANTE A LOS EFECTOS DE ESTABLECER LA OBLIGACIÓN DE INTEROPERABILIDAD.

No obstante el silencio de la Constitución, el contenido de la obligación de interoperabilidad se ha construido a partir de las disposiciones antes señaladas y lo previsto en la ley analizados a la luz de la jurisprudencia de los tribunales ordinarios.

En sede legal debemos atender al DFL Nº 1, LOCBGAE, en cuanto establece que la Administración del Estado debe observar el deber de coordinación, entre otros, para lo que debe propender a la unidad de acción y evitar la duplicación o interferencia de funciones.[4] Asimismo la ley Nº 21.180 de 2019, sobre Transformación Digital del Estado, en cuanto modifica la ley Nº 19.880 sobre procedimientos administrativos para consagrar el principio de coordinación como uno de carácter general para todos los procedimientos que se tramiten por medios electrónicos. Asimismo, los conceptos de procedimiento y expediente electrónico ya consagrados en la ley N° 19.880 cobran relevancia a los efectos de nuestra investigación.

En sede jurisprudencial, son fundamentales algunos pronunciamientos de la Corte Suprema que han resignificado el principio constitucional de coordinación. A modo ejemplar, la Corte ha sostenido que este principio exige "[…] la disposición metódica y racional de las actividades que desarrollan los órganos administrativos, individualmente y en su conjunto, para el cumplimiento más eficiente y eficaz de la función administrativa y la mayor satisfacción de las necesidades colectivas a cargo del Estado, con el menor costo financiero y social posible".[5]

Adicionalmente, a raíz de la relación entre el carácter unitario del Estado y el deber de coordinación, la Corte Suprema ha sostenido que "[…] no obstante que el Estado de Chile

[4] Artículos 3º y 5º de la LOCBGAE.
[5] SCS Nº 34.536-2017, considerando 7º.

ejecuta sus funciones a través de distintos órganos, es uno solo, por lo que debe haber un esfuerzo serio de coordinación entre las distintas instituciones, […] debiendo actuar mancomunadamente con el fin de no perjudicar a las personas, a cuyo servicio se encuentra el Estado conforme a lo preceptuado en el artículo 1° inciso 4° de la Constitución Política de la República".[6]

Por último, a propósito de la necesidad de que el Estado tenga recursos suficientes para satisfacer su finalidad, la Corte Suprema ha resuelto que "[l]a insuficiencia de recursos económicos está siempre presente y ella impide dar una mejor satisfacción a las necesidades colectivas por lo que se hace necesaria la coordinación de los servicios de la administración a fin de maximizar los recursos escasos en procura de la finalidad principal a que está obligado el Estado, esto es, alcanzar el bien común".[7] Al respecto, es menester tener presente que, en el Capítulo I sobre Bases de la Institucionalidad, la Constitución sí establece las bases jurídico-políticas desde las que concibe la regulación de fichas clínicas, además de prever que deberán ser respetadas en todo momento por el operador jurídico.

En efecto, el artículo 1º inciso cuarto, consagra que el fin del Estado corresponde al servicio de la persona humana y que su finalidad es promover el bien común con pleno respeto a los derechos y garantías constitucionales. En ese contexto, se erige, además, la obligación del Estado de brindar protección a la población en un sentido amplio (de acuerdo con el inciso final de la precitada disposición). Por consiguiente, tanto el fin (servicio) como la finalidad (bien común) del Estado serán las directrices básicas a las que deberá ajustarse la Administración al momento de coordinar y controlar las acciones relacionadas con la salud. En sede legislativa, así como en el desarrollo de las políticas públicas relativas a fichas clínicas, deberá adoptarse las medidas que tiendan a la satisfacción de estos criterios elementales, porque de lo contrario la acción de los órganos respectivos adolecería de vicios de constitucionalidad. A ello debemos sumar lo previsto en la modificación al artículo 19 Nº 1 CPR, en tanto establece que el desarrollo científico y tecnológico están al servicio de la persona humana, de lo cual se desprende que las políticas públicas de salud digital deberán considerar la interoperabilidad de la información de salud, como una herramienta consustancial a la concreción del derecho a la salud, reconocido constitucionalmente.

[6] SCS Nº 31.594-2018, considerando 4º.
[7] SCS Nº 34.536-2017, considerando 7º.

3.- LA REGULACIÓN LEGAL Y REGLAMENTARIA DE LA GESTIÓN DE LA FICHA CLÍNICA.

El grueso del marco normativo de fichas clínicas se encuentra contenido en la LDDP y el Decreto Nº 41, del Ministerio de Salud, de 2012, que reglamenta su tratamiento.

A. LEY 20.584, QUE "REGULA LOS DERECHOS Y DEBERES DE LOS PACIENTES EN RELACIÓN CON ACCIONES VINCULADAS A SU ATENCIÓN DE SALUD".

La ley N° 20.584, en vigencia desde el año 2012, define en su artículo 12 la ficha clínica como "el instrumento obligatorio en el que se registra el conjunto de antecedentes relativos a las diferentes áreas relacionadas con la salud de las personas, que tiene como finalidad la **integración de la información necesaria** en el proceso asistencial de cada paciente" (el destacado es nuestro). Luego, la LDDP, establece los requisitos que debe cumplir la ficha clínica.

No habiendo otra definición de la ficha clínica, siempre que otra ley o cuerpo reglamentario mencione este instrumento, deberá entenderse en los términos de la disposición precitada.

Destacamos en el concepto el término "integración de la información necesaria", porque entendemos que esta finalidad emana directamente del mandato constitucional de garantizar la salud de la persona, a través de la realización de las acciones y prestaciones de salud que requiera. Lógicamente, el cumplimiento de dicho deber no se verifica cuando la información de salud de las personas está diseminada en diversas fichas clínicas que carecen, entre ellas, de vasos comunicantes, o incluso cuando no cuentan con un soporte electrónico.

Es necesario precisar que existe una cierta tendencia a emplear indistintamente los conceptos de ficha e historia clínicas —incluso a nivel reglamentario— para referirse al objeto regulado en el artículo 12, pero se trata de nociones diferentes e independientes entre sí. Mientras la ficha clínica es el continente en el cual se registra la información, la historia clínica apunta más bien al contenido, esto es al "conjunto de antecedentes relativos a las diferentes áreas relacionadas con la salud de las personas" en los términos del aludido precepto. De esta manera, podemos apreciar que la historia clínica se aparta del instrumento que le otorga entidad material para apuntar más bien hacia un relato o crónica. En otras palabras, la historia clínica, a diferencia de la ficha, "corresponde a la cronología médica de una persona, toda su historia, que se construye o más bien descubre en un

proceso, de carácter comunicacional entre el facultativo y el paciente, obteniendo la información patológica de una persona".[8]

De acuerdo con lo anterior, el ideal es que toda la historia clínica de las personas conste en las respectivas fichas clínicas. Sin embargo, por razones de distinta naturaleza —negligencia, caso fortuito, cambio de prestador u otras—, ambos conceptos no siempre serán equivalentes, lo que nos obliga a emplear en el presente estudio estos términos según el sentido que se ha explicado anteriormente, por tratarse de cuestiones relacionadas, pero distintas. Solamente se utilizará, de modo indistinto, el concepto de ficha clínica o médica para hacer referencia a lo prescrito por el artículo 12 de la ley.

Esta misma disposición establece que la ficha clínica puede ser configurada en cualquier soporte —papel, electrónico u otro— siempre y cuando se verifiquen taxativamente determinados requisitos o condiciones mínimas que correspondan a: a) registros completos; b) acceso oportuno; c) conservación; d) confidencialidad; e) autenticidad del contenido; y, f) auditabilidad de todos los cambios efectuados.

Al respecto, es posible observar que el legislador fue consciente de la velocidad del avance tecnológico y, debido a ello, prefirió regular el soporte de la ficha clínica sobre la base de ciertos requisitos, evitando inclinarse por uno en particular que pudiere caer, de un momento a otro, en la obsolescencia.

Finalmente, el artículo 12 cierra asentando que "toda la información que surja, tanto de la ficha clínica como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que sean sometidas las personas constituye un dato personal de carácter sensible, de acuerdo con el artículo 2º letra g) de la ley 19.628".

En palabras sencillas, esto quiere decir que cualquier antecedente que se registre durante la atención que reciba un paciente, así como toda la información que derive de la prestación otorgada, se incluye dentro de la categoría de datos sensibles. La importancia de esta categorización consiste en que tiene un régimen jurídico más estricto que será analizado al momento de abordar las prerrogativas de la LPVP.

[8] ETEROVIC BARREDA, Pablo. Acceso a la ficha clínica en el derecho chileno. Ediciones jurídicas de Santiago, 2019. p. 23.

Por otra parte, y de acuerdo con el artículo 13, la ficha debe ser almacenada por el prestador por un periodo de, al menos, quince años. En ese lapso, el prestador será, además, responsable de su administración, conservación y reserva.

Esta disposición también prohíbe que terceros no relacionados directamente con la atención de salud tengan acceso a la información contenida en la ficha clínica, por lo que no tendrán acceso a su contenido el personal de salud y administrativo del prestador que no estén vinculados con la atención de la persona.

La norma de la ley N° 20.584 es concordante con el hecho de que toda la información de salud de la persona es dato sensible, en los términos de la ley 19.628 y con el hecho de que esta información no proviene de fuentes de libre acceso público y, en consecuencia, no habría fundamento legal para dar acceso a esta información a funcionarios ajenos a la atención de salud.

No obstante, dicha regla no es absoluta, y es el mismo artículo 13 el que prevé aquellos casos en que terceros pueden acceder total o parcialmente a una copia o parte de la ficha clínica, siempre previa solicitud expresa de ellos. En estos casos, verificadas las condiciones establecidas en la ley, el prestador requerido estará obligado a otorgar acceso o copia a todo o parte de la ficha al requirente.

Tratándose del titular de la ficha clínica o su representante legal, sólo exige la solicitud de acceso. Tratándose de los herederos, en cambio, habrán de acreditar el fallecimiento y la calidad de tales.

En el caso de terceros, distintos de los herederos, para acceder a la ficha, además de realizar la solicitud correspondiente, deberán ser autorizados por el titular mediante un poder simple otorgado ante notario. Este resguardo se explica a la luz del carácter sensible de esta información, cuyo acceso irrestricto en favor de terceros, posicionaría al titular en la más absoluta indefensión.

En materia judicial, los tribunales de justicia siempre pueden acceder a la ficha clínica cuando la información contenida en esta guarde relación con causas que estén en actual tramitación y que así sea requerido. En cambio, los fiscales del Ministerio Público o abogados —querellantes o defensores— deben solicitar el acceso al juez competente,

quien podrá autorizarlo cuando la información esté vinculada directamente con las investigaciones o defensas que tengan asignadas.[9]

Por último, el ISP puede solicitar el acceso total o parcial a fichas clínicas en el cumplimiento de sus funciones.[10]

Ahora bien, como contrapartida, todos estos legitimados activos deben adoptar las providencias necesarias para asegurar la reserva de la identidad del titular, de los datos sensibles y para que el tratamiento se ajuste —exclusivamente— a finalidad invocada al requerir la información, según obliga el inciso final del artículo 13.

Con todo, estas providencias no constituyen una excepción al deber general de los prestadores de velar por la confidencialidad, disponibilidad e integridad de las fichas clínicas que administren durante el plazo que lo hagan, sino que más bien regula, dentro del marco de la confidencialidad, quienes estarán facultados para acceder a la información que consta en la ficha.

Es importante tener presente que existen otros casos, disgregados en diversos cuerpos legales, en que otros funcionarios u organismos públicos —distintos a los enunciados en el

[9] Cabe señalar que, respecto de las letras c) y d), el TC en causa Rol Nº 2.159-2012, ejerciendo sus funciones de control preventivo, declaró inconstitucional la redacción original despachada por el Congreso Nacional.
En efecto, la primera enmienda señalaba: "c) A los tribunales de justicia, siempre que la información contenida en la ficha clínica se relacione con quien tenga el carácter de parte o imputado en las causas que estuvieren conociendo." El TC declaró inconstitucional la limitación de esta atribución solo para las partes y al imputado, argumentando que "en un proceso puede ser necesario solicitar antecedentes no sólo de quienes tienen el rol propiamente de parte o imputado en el mismo —sea civil o penal—, sino también de otras personas que no necesariamente revistan dicho carácter, pero que se vinculen de manera relevante con el desarrollo del proceso jurisdiccional, todo lo cual puede ser estrictamente indispensable para resolver la litis".
Por su parte, la segunda norma establecía lo siguiente: "d) A los fiscales del Ministerio Público y a los abogados defensores, previa autorización del juez competente, cuando la información se vincule directamente con las investigaciones o defensas que tengan a su cargo.". Aquí el TC declara inconstitucional la expresión "defensores" basándose en que "[…] no resulta constitucionalmente aceptable limitar la petición de información del contenido de la ficha clínica exclusivamente al Ministerio Público y a los abogados defensores de los imputados, considerando que también tienen protección de la Ley Fundamental, en cuanto al ejercicio de la acción penal, el ofendido por el delito y las demás personas que determine la ley".

[10] Ello sin perjuicio de que el dictamen Nº 38.604-2013 de CGR ha declarado que se encuentran autorizados para acceder a la ficha clínica de un paciente, además de las personas y organismos indicados en el artículo 13 LDDP, aquellos que hayan sido habilitados por otros cuerpos legales; puesto que el artículo 10 LPVP permite que los datos sensibles sean objeto de tratamiento, cuando la ley lo autorice, exista consentimiento del titular o sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares, situaciones que se configuran respecto de diferentes entidades, tales como el MINSAL, la SUPERSALUD y su Intendencia de Prestadores de Salud, y el FONASA, entre otras, todas ellas autorizadas, como ha podido apreciarse, mediante el aludido decreto con fuerza de ley Nº 1 de 2005.

artículo 13 de la LDDP— pueden acceder a fichas clínicas; estos serán abordados exhaustivamente en el acápite 5º de este capítulo. Sin embargo, podemos anticipar que algunos de ellos son el Ministerio de Salud, el INDH y las FOS, entre otros.

La ley reconoce, en el artículo 14, el derecho de los pacientes a consentir o rechazar cualquier procedimiento o tratamiento vinculado a su atención de salud. Únicamente se excluyen aquellos casos en los que el rechazo pueda tener como objetivo la aceleración artificial de la muerte, la eutanasia o el auxilio al suicidio, porque constituyen materias u objetos respecto de los cuales el ordenamiento jurídico —vigente— no permite disponer. Al respecto, resulta pertinente acotar que existe un PDL en segundo trámite constitucional que, de aprobarse, derogaría tácitamente estas limitantes[11].

No obstante, mientras este PDL no se transforme en ley, el artículo 16 continuará regulando el restringido margen de acción que la ley le reconoce a las personas en estado terminal.

Ahora bien, la aceptación del paciente, por regla general, podrá ser expresada de manera verbal, en cuyo caso no será obligatorio dejar registro clínico. Sin embargo, en aquellos casos en que se apliquen procedimientos que conlleven un riesgo relevante y conocido para la salud —intervenciones quirúrgicas o procedimientos diagnósticos o terapéuticos de carácter invasivos, según indica la ley—, la aceptación o el rechazo deberá necesariamente constar por escrito en la ficha clínica, lo que se demostraría con la firma en el documento explicativo del procedimiento o tratamiento.

Esta obligación exige dejar registro tanto del hecho de la entrega como del contenido de la información que se dio a conocer, así como de cada uno de los contenidos mínimos que componen el derecho del paciente a recibir información por parte del profesional tratante que están establecidos en el artículo 10.

Tratándose de NNA, y sin perjuicio de las facultades de los padres o representantes legales para consentir en su nombre, el artículo 14 obliga a que sean informados y oídos tomando en consideración su edad, madurez, desarrollo mental y estado afectivo y psicológico. Esto se complementa con lo dispuesto en la ley Nº 21.067, que crea la Defensoría de los Derechos de la Niñez, particularmente en los artículos 4º letras b) y e), 8 y 16, en virtud de los cuales esta institución posee legitimación activa para acceder a las fichas clínicas de

[11] PDL sobre el “Derecho a optar voluntariamente para recibir asistencia médica con el objeto de acelerar la muerte en caso de enfermedad terminal e incurable” (boletín 7736-11).

los NNA a efectos de velar por sus derechos, así como también de perseguir a terceros en su salvaguarda.

Con todo, la ley sí contempla excepciones en las que no se requiere contar con una manifestación de voluntad del paciente para someterse a un procedimiento o tratamiento vinculado a su atención de salud. Entre estas destaca la hipótesis en que la falta de intervención, procedimiento o tratamiento suponga un riesgo para la salud pública por ser especialmente atingente en tiempos en los que el COVID-19 todavía apremia. En estos casos, el profesional tratante debe dejar constancia en la ficha clínica que está invocando esta causal, regulada por los artículos 15 y 16.

Adicionalmente, la ley aborda la ficha clínica con ocasión de los derechos de las personas con discapacidad psíquica e intelectual, en relación con tratamientos de salud, en el artículo 23, que regula la reserva y restricción en el acceso de información del paciente o titular sobre su ficha clínica debido a los efectos negativos que esa información pudiera tener en su estado mental podría provocar en su estado mental. Adicionalmente, impone la obligación de que el profesional tratante informe al representante legal del paciente —o a la persona bajo cuyo cuidado se encuentre— las razones médicas que justifican tal medida.

Por último, en relación con este tipo de pacientes, la ley establece dos hipótesis de registro obligatorio. La primera corresponde a las medidas de aislamiento o de contención física y farmacológica que deban aplicarse a su respecto, caso en el cual, en un intento por generar condiciones para que el empleo de estas medidas sea reducido y proporcional a la conducta del paciente y —más importante aún— acordes a la dignidad de la persona, el legislador incorporó la obligación de que todo lo obrado con motivo del empleo del aislamiento o la sujeción conste por escrito en la ficha clínica.

La segunda, consiste en el deber de comunicar el empleo de estas medidas a la Autoridad Sanitaria Regional, lo cual surge a raíz de los tratamientos involuntarios, debido a que la ley contempla el deber de registro obligatorio en la ficha clínica como uno de los requisitos insalvables para que estos sean procedentes respecto de personas con discapacidad psíquica.

B. CÓDIGO SANITARIO.

El Código Sanitario establece que tanto la receta y su contenido, los análisis y exámenes de laboratorios clínicos y los servicios prestados relacionados con la salud son reservados y considerados sensibles (art. 101 inciso noveno). Asimismo, al clarificar que los registros, libros, fichas clínicas y documentos de los establecimientos destinados a la observación de enfermos mentales y de quienes presentan dependencias de drogas u otras substancias son también reservados (art. 134).

En tercer lugar, establece la regulación de los sumarios sanitarios; un procedimiento de aplicación general que —como hemos visto— tiene aplicación frente a la transgresión del régimen jurídico de las fichas clínicas (Libro X).

Recordemos, en todo caso, que el principio general de confidencialidad no es absoluto pues en diversos cuerpos jurídicos están contempladas situaciones excepcionales, por ejemplo, en el caso de los organismos públicos que para el adecuado ejercicio de sus competencias requieren necesariamente acceder a determinada información sensible, como podrían ser tratándose de aquellos del sector salud (ley 20.584).

C. DFL Nº 1 DE 2006 DEL MINSAL.

La relevancia de este cuerpo normativo surge porque contempla dentro de las funciones del Ministerio —específicamente en el artículo 4º literal 5º— el tratamiento de datos personales o sensibles, con el fin de proteger la salud de la población o para determinar y otorgar de beneficios de salud. Incluso, para ejercer esta potestad, puede requerir de las personas naturales o jurídicas, públicas o privadas, la información que fuere necesaria, en la medida en que respete las normas de la ley N° 19.628 y las normas sobre secreto profesional. En un sentido similar, este decreto con fuerza de ley confiere atribuciones a la SUPERSALUD para solicitar a los prestadores, públicos o privados, las fichas clínicas u otros antecedentes médicos necesarios para resolver reclamos y también para decidir la procedencia de beneficios (art. 115 Nº 7 y art. 110 Nº 17). Lo propio prescribe respecto del ISP, que puede acceder a la información proporcionada por el prestador (art. 189). Por último, establece en el artículo 134 bis, que “los prestadores de salud, las instituciones de salud previsional, el FONASA u otras entidades, tanto públicas como privadas, que elaboren, procesen o almacenen datos de origen sanitario no podrán vender, ceder o transferir, a cualquier título, bases de datos que contengan información sensible respecto

de sus usuarios, beneficiarios o pacientes, si no cuentan para ello con el consentimiento del titular de tales datos, en los términos previstos en la ley N° 19.628 o en otras normas especiales que regulen dicha materia, salvo que se trate del otorgamiento de los beneficios de salud que les correspondan, así como del cumplimiento de sus respectivos objetivos legales, para lo cual no se requerirá de dicho consentimiento".

D. Decreto Nº 41, que "Aprueba el Reglamento Sobre Fichas Clínicas".

Adicionalmente, el Decreto Nº 41 de MINSAL, aprueba el Reglamento sobre Fichas Clínicas, publicado en 2012 con solo unos meses de diferencia respecto de la ley N° 20.584.

Sus disposiciones se estructuran en base a tres títulos; el primero sobre Disposiciones Generales, el segundo referente al Almacenamiento y Protección y el último relativo a la Administración, Acceso y Eliminación.

En primer lugar, el Título I, delimita el objeto reglamentario en su artículo 1º, señalando que consiste en "regular las condiciones de elaboración, contenido, almacenamiento, administración, protección y eliminación de las fichas clínicas de todas las personas que reciben atención de salud y, además de los pacientes, es aplicable para todos los prestadores de salud, tanto institucionales como individuales, del ámbito público y privado". Se sienta por tanto la universalidad de sus disposiciones, en tanto que todo paciente debe contar con una ficha y todo prestador queda bajo sus normas, con independencia de si se trata de un prestador público o privado, institucional o individual (art. 4º).

En seguida, los artículos siguientes reiteran y refuerzan las normas de la LDDP, referentes a la definición de la ficha clínica (art. 2), soportes (art. 2 inciso segundo), categorización de datos personales (art. 2 inciso final) y deber de registro (art 3), distinguiendo si la entrega de la información es escrita o verbal. Tratándose de la información verbal, se establece la obligación de hacer constar en la ficha el hecho de haber sido efectivamente proporcionada al paciente.

Sin embargo, estas normas no implican que respecto de una persona exista solamente una ficha clínica, principalmente por dos razones. La primera está contenida en el propio artículo 4º, que autoriza a los establecimientos de atención cerrada, hospitales, clínicas y demás, a mantener fichas clínicas propias en algunos servicios o unidades especializadas. Para ello, el único requisito es que en la ficha clínica central se consignen las fechas de atención, el

profesional que la prestó, la evaluación diagnóstica y los medicamentos prescritos con sus dosis y plazos de administración. La segunda porque dicha declaración, si bien reconoce una ficha clínica por paciente atendido, nada establece sobre medidas tendientes a lograr la uniformidad e interconexión de la historia clínica, ni menos a establecer su interoperabilidad. Esto tiene por efecto que esta obligación sea poco útil para la práctica médica y mejor atención de los pacientes, al menos en sus actuales términos.

Ahora bien, el reglamento añade, a las características legales de la ficha clínica que abordamos al estudiar el artículo 12 de la ley, otras referentes a su nitidez y cronología. En este sentido, la construcción de la ficha, más allá de su soporte, debe ser llevada a cabo en forma clara y legible, conservando su estructura en forma ordenada y secuencial. Adicionalmente, en el artículo 6º del reglamento se contemplan una serie de antecedentes mínimos y perentorios que deben constar en la ficha clínica:

ANTECEDENTES MÍNIMOS FICHA CLÍNICA SEGÚN DECRETO Nº 41 DE 2012	
Identificación actualizada del paciente	Nombre completo, número y tipo de documento de identificación (cédula de identidad, pasaporte, u otro), sexo, fecha de nacimiento, domicilio, teléfonos de contacto y/o correo electrónico, ocupación, representante legal o apoderado para fines de su atención de salud y sistema de salud al que pertenece.
Individualización de la ficha y del prestador	Número de identificación de la ficha, fecha de su creación, nombre o denominación completa del prestador respectivo, indicando cédula de identidad o rol único tributario, según corresponda.
Registro cronológico y fechado de todas las atenciones de salud recibidas	Esto incluye a consultas, anamnesis, evoluciones clínicas, indicaciones, procedimientos diagnósticos y terapéuticos, intervenciones quirúrgicas, protocolos quirúrgicos u operatorios, resultados de exámenes realizados, interconsultas y derivaciones, hojas de enfermería, hojas de evolución clínica, epicrisis y cualquier otra información clínica. Además, en caso de agregar documentos, en forma escrita o electrónica, cada uno debe llevar el número de la ficha.
Decisiones adoptadas por el paciente o respecto de su atención	A modo referencial están contemplados los consentimientos informados, rechazos de tratamientos, solicitud de alta voluntaria, altas disciplinarias y requerimientos vinculados a sus convicciones religiosas, étnicas o culturales, en su caso.

TABLA 1. ELABORACIÓN PROPIA.

La confirmación de datos de identificación del paciente constituye una obligación del personal tratante cada vez que tenga lugar una nueva atención, junto con la modificación de todos aquellos que han variado desde que se produjo la última consulta. Asimismo, por más evidente que aparezca, una vez satisfechas estas exigencias, el personal deberá añadir los nuevos registros que resulten de la consulta e individualizar, por medio de una firma, al profesional que la otorga (artículo 13).

Por otro lado, el Título II del Reglamento, referente al Almacenamiento y Protección de las fichas clínicas, comienza con el artículo 8º, cuya importancia redunda en la distinción de estándares según el soporte de que se trate. De esta manera, las fichas con soporte electrónico deben cumplir los siguientes requisitos: respaldar la información en cada proceso de incorporación de los documentos; contar con una copia de seguridad en el lugar de operación de los sistemas de información y otra distinta en un centro de almacenamiento de datos electrónicos que tenga un estricto control de acceso y registro de entrada y salida de respaldos; utilización de medidas de seguridad y barreras de protección frente a terceros no autorizados; y, finalmente, sustitución de la información por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programadas.

Las fichas con soporte en papel deben ser almacenadas en un archivo único y centralizado, ordenadas con características que permitan su ubicación expedita; debe ser posible su mantención, conservación y reposición de carátulas en casos de deterioros; los extravíos y omisiones de documentos deben poder ser controlados; los archivos deben estar ordenados en un orden secuencial por números de fichas o letras; debe existir un sistema de constancia de solicitudes de acceso a las fichas; y mantener un registro de entrada y salida de las fichas con indicación del destinatario responsable y fechas de pedido y de devolución.

Finalmente, el Título III y final del Reglamento Nº 41 se refiere a la Administración, Acceso y Eliminación (arts. 9 a 14), una materia que la ley —en su artículo 13— autoriza expresamente para que sea regulado por esta vía. En efecto, el artículo 9º comienza haciéndose cargo de la Administración al establecer que la forma de gestionar las fichas clínicas deba ser centralizada. Esto aseguraría la confidencialidad; el acceso controlado solo de aquellas personas que puedan tomar conocimiento de sus registros y consignar nuevos datos en ella; el registro de las fechas y personas que han accedido y el uso de medidas de seguridad destinadas a evitar los accesos de terceros no directamente relacionados con la atención de salud del titular de la ficha, incluido el personal de salud y administrativo del prestador.

Luego, los artículos 10 y 11 replican los contenidos del artículo 13 LDDP, porque, respectivamente, aluden al acceso por parte de terceros distintos del titular de la ficha clínica y al almacenamiento. Sin embargo, conviene hacer notar que —a diferencia de la ley—, el artículo 10 considera a organismos distintos del ISP y el 11, por su parte, añade

que el plazo de quince años se contará desde el último ingreso de información que experimente la ficha clínica.

Por otro lado, en conformidad al artículo 12, la eliminación de las fichas clínicas procederá tan pronto transcurra el plazo de conservación. La norma dispone que dicho procedimiento se puede llevar a cabo a través de medios necesarios propios o ajenos, debiendo asegurar la confidencialidad de la información y su efectiva destrucción. No obstante, previo a que se verifique la eliminación, los prestadores deben levantar un acta donde quede constancia de todo lo obrado e incluir, al menos, el nombre del paciente y el número de su ficha clínica.

En el caso de los prestadores institucionales, el reglamento distingue según se trate de entidades públicas o privadas. En el primer caso, para llevar a cabo la eliminación de fichas clínicas es necesario que exista una resolución previa que lo autorice, mientras que en el caso de las segundas deberán protocolizar el acta ante notario. El reglamento finaliza con el establecimiento de la responsabilidad del prestador en cuanto a que la conservación y reserva de la ficha clínica cesa en el momento en el que se verifica el procedimiento de eliminación. Asimismo, encarga el control y fiscalización de esta normativa a la Intendencia de Prestadores de la SUPERSALUD.

E. DECRETO Nº 38, QUE "APRUEBA REGLAMENTO SOBRE DERECHOS Y DEBERES DE LAS PERSONAS EN RELACIÓN CON LAS ACTIVIDADES VINCULADAS CON SU ATENCIÓN DE SALUD".

Como complemento, es necesario mencionar que el Decreto Nº 38 de 2012, que desarrolla en el Título II todos los derechos consagrados por la LDDP, destacando particularmente el derecho a recibir un trato digno (artículos 5º a 9º del reglamento y 5º de la ley).

Pues bien, en conformidad a este derecho es obligatorio el respeto y protección de la vida e intimidad de las personas, cuestión no menor considerando que a la fecha de publicación del Decreto Nº 38 aún no existía la garantía fundamental de protección de los datos personales (2018), sin perjuicio que esta norma se explica por lo dispuesto en las normas del Código Sanitario, introducida con ocasión de lo previsto en la ley N° 19.628.

Concretamente, la inclusión de este mandamiento implica que las imágenes del cuerpo del paciente —o parte de este— que sean necesarias para la labor clínica, deberán ser conservadas con la debida reserva.

Por último, el Decreto Nº 38 establece, en el artículo 15, que la configuración, almacenamiento, protección y eliminación de la ficha clínica, así como la administración y reserva de la información que en esta se vierta, se rigen por las disposiciones reglamentarias especiales que al efecto se dicte. Es decir, por el Decreto Nº 41 que abordamos anteriormente.

4.- MARCO JURÍDICO DE PROTECCIÓN DE DATOS PERSONALES PARA LA FICHA CLÍNICA.

En materia de Protección de datos personales, adicionalmente a las normas constitucionales antes señaladas, debemos analizar la ley Nº 19.628 de 1999, Sobre Protección de la Vida Privada.

A. LEY Nº 19.628.

La ley N° 19.628, se dictó el año 1999 anclada en el artículo 19 N°4 de la Constitución Política de la República. A la época de su dictación, el texto constitucional incluía la protección de la vida pública, privada y la honra de las personas. Luego, en los procesos de reforma constitucional, en primer lugar, se eliminó la protección de la vida pública y más tarde se agregó la protección de datos personales.

Entre los preceptos de la ley N° 19.628, debemos tener a la vista la definición de datos sensibles, que se conceptualizan como “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como […] los estados de salud físicos o psíquicos […]”.

Esta definición es fundamental por cuanto su significado aplicará cada vez que otros cuerpos jurídicos hagan referencia al concepto de datos sensibles, como es el caso del Código Sanitario, la LDDP y su Decreto Nº 41.

Ahora bien, en relación con esta categoría de datos, la regla general es que su tratamiento esté prohibido, salvo en tres hipótesis: cuando la ley lo autorice; exista el consentimiento del titular o bien sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Para estos efectos, es importante entender que por tratamiento de datos nos referimos a “cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter

automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma", según lo define el artículo 2º letra o) de la LPVP.

En este sentido, el tratamiento de datos sensibles por cualquier persona —natural o jurídica— debe ser realizado siempre respetando tanto la ley como las finalidades permitidas por el ordenamiento jurídico. Más aún, los tratamientos de datos personales no deben entorpecer u obstaculizar el pleno ejercicio de los derechos fundamentales de los titulares, así como las facultades que la ley les reconoce.

Adicionalmente, la ley regula las facultades de los titulares de datos —en este caso de salud—, las que constituyen las principales herramientas que el ordenamiento jurídico brinda a las personas para el ejercicio y cautela de sus derechos. Estas atribuciones se sintetizan en el acrónimo ARCO, conformado a través de las iniciales de los vocablos Acceso, Rectificación, Cancelación (supresión, eliminación, olvido), y Oposición, además del bloqueo, como una herramienta al servicio de estos derechos.

Estos derechos se consagran en los artículos 3º y 12 de la LPVP. Dichos derechos se caracterizan por ser gratuitos, no susceptibles de ser limitados por acto o convención alguna y pueden ser ejercidos ante el responsable del registro o banco de datos. Tratándose de bancos de datos compartidos por distintos órganos el titular podrá ejercerlos respecto de cada uno de ellos.

En todo caso, los derechos ARCO no proceden cuando tengan por efecto impedir o entorpecer el debido cumplimiento de las funciones fiscalizadoras de un organismo; afecten la reserva o secreto establecidas en una ley o reglamento o bien, atenten contra la seguridad de la nación o el interés nacional.

Ahora bien, cuando sea entorpecido u obstaculizado el ejercicio de los derechos ARCO por haberse invocado causales distintas a las descritas o por no existir pronunciamiento dentro de dos días por parte del responsable del registro o banco de datos, cabe la posibilidad de recurrir a la justicia civil interponiendo una acción de amparo denominada *habeas data*. Esta acción es cautelar, por consiguiente, nada impide que las personas acudan a la justicia ordinaria cuando sufran un daño patrimonial o moral producto del tratamiento indebido de

sus datos. Ello por cuanto, en estos casos, la causa de pedir es el resarcimiento pecuniario, mientras que lo propio de las acciones cautelares es el restablecimiento del derecho.

Sin embargo, esta distinción resulta teórica, puesto que en la práctica se impone el uso de la acción de protección consagrada en el artículo 20 de la Carta Magna, básicamente porque exige menos requisitos que la *habeas data*; por ejemplo, no requiere del patrocinio de un abogado. Por su parte, respecto de acciones que persiguen el resarcimiento económico, estas adolecen y comparten las críticas que la doctrina realiza sobre las acciones civiles, que se caracterizan por su sosegada tramitación. Hasta aquí, cabe acotar que todo lo que hemos sostenido en relación con la LPVP está corroborado y complementado por la recomendación del CPLT sobre PDP por parte de los órganos de la Administración del Estado, vigente desde el 7 de diciembre de 2020.

Previo al análisis de la Recomendación, es necesario considerar que LPVP no designa ni regula una autoridad fiscalizadora de sus prescripciones, cuestión que, considerando los problemas prácticos que suscitan los mecanismos o recursos que la ley entrega en la actualidad, las personas imploran para velar por su derecho a la autodeterminación informativa.

Tanto es así que solo el año 2008, con la publicación de la ley Nº 20.285, sobre acceso a la información pública, el legislador contempló al CPLT como la autoridad encargada de fiscalizar exclusivamente el cumplimiento de la LPVP por los organismos públicos (art. 33 letra m). Antes, dicha labor era realizada residualmente por la CGR.

En este contexto, estimamos que en el presente prácticamente no existen incentivos para que los particulares cumplan la LPVP que, por lo demás, en sí misma no es capaz de brindar un estándar de protección suficiente para las personas, sobre todo si se considera lo que otros países —incluso de nuestra región— han legislado en la materia. Esta afirmación se ve corroborada porque existe una autoridad fiscalizadora con competencia respecto de los privados, sin perjuicio de que la institucionalidad debiera satisfacer otros requisitos, como la independencia, tal y como se exige en la Carta Europea de Derechos Fundamentales.[12]

[12] Artículo 8º de la Carta Europea de Derechos Fundamentales.
"Protección de datos de carácter personal.
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

Refiriéndonos directamente al objeto regulatorio de la recomendación del CPLT, es necesario acotar que esta reitera las normas que la ley establece acerca de los datos sensibles, con la diferencia de que agrega la obligación de adoptar medidas de seguridad adecuadas al nivel de sensibilidad y riesgo.

Asimismo, incluye explícitamente dentro del concepto de datos sensibles a aquellos que corresponden a DPS, despejando cualquier duda que pudiere existir al respecto. En efecto, al sistematizar los datos personales sensibles entre aquellos que se refieren a las características físicas, morales o a hechos o circunstancias de la vida privada o intimidad de una persona, tiene por mérito ubicar a los relativos a la salud dentro de la primera categoría. A su vez, la recomendación sobresale por delimitar y precisar el alcance de tratamientos realizados para la determinación u otorgamiento de beneficios de salud, puesto "únicamente podrán hacer uso de esta disposición aquellos organismos públicos que otorguen "beneficios de salud" en el ejercicio de sus funciones y respecto de materias de su competencia".[13]

No obstante, todos estos avances no pasan de ser meras declaraciones al tomar en cuenta que el CPLT no está dotado de un catálogo de medidas coercitivas, razón por la cual no tiene manera de obligar al cumplimiento de la ley, de ahí que "recomiende". Además, como hemos mencionado, de antemano su marco de acción es limitado al ceñirse exclusivamente a los organismos públicos y no a los particulares.

Para finalizar este acápite, es menester tener en consideración que el PDL que reforma la LPVP incorpora, dentro del catálogo de derechos disponibles para el titular, el derecho a la portabilidad. En virtud de este, el titular puede "solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y común, que permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos".[14] Incluso, en caso de que este derecho sea impedido u obstaculizado, considera dicha conducta como una infracción grave, que tiene aparejada una sanción de multa de 101 a 5.000 unidades tributarias mensuales.[15]

---

3. El respeto de estas normas quedará sujeto al control de una autoridad **independiente**" (el destacado es nuestro).

[13] Recomendación CPLT sobre "Protección de datos personales por parte de los órganos de la Administración del Estado", literal 8º, parte final.

[14] Artículos 2º letra t) y 4º del PDLPDP.

[15] Op. Cit. artículo 35.

Por último, cabe añadir que recientemente el Congreso Nacional sancionó una ley que regula en otro ámbito a la portabilidad: la ley Nº 21.236 de 2020 que "regula la portabilidad financiera", la cual sigue el camino iniciado por una ley pionera en este ámbito, como lo es la Nº 20.471 de 2010, que "obliga a los concesionarios de servicio público telefónico a implementar un sistema de portabilidad numérica".

En este contexto, es de esperar que la portabilidad se siga haciendo extensible a diversos rubros, incluyendo a la PDP, tanto a nivel general como en concreto, a las fichas clínicas.

B. Decreto N° 779, que aprueba el reglamento de registro de bancos de datos personales a cargo del Estado.

Los sistemas que albergan las fichas clínicas en instituciones públicas son registros o bancos de datos, y, en estas circunstancias, están sujetos al deber de registro consagrado en el artículo 24 de la ley N° 19.628 y reglamentado por el Decreto Nº 779, de 24 de agosto de 2000, del Ministerio de Justicia.

En este acápite, por lo tanto, nos referiremos a las normas legales y reglamentarias asociadas al tratamiento de datos por parte de los organismos públicos, especialmente en lo relativo a los prestadores públicos del área de la salud.

Todos los órganos del Estado y organismos públicos indicados en el inciso segundo del artículo 1º de la ley 18.575, deben llevar a cabo el registro de los bancos de datos personales de los que son titulares. La inscripción debe considerar el nombre del banco de datos personales, el organismo público responsable, RUT, fundamento jurídico de la existencia, finalidad, tipos de datos almacenados y una descripción del universo de personas que comprende, sin perjuicio de que esta materia también está definida en el artículo 22 LPVP. El Registro Civil, por su parte, debe entregar al organismo público responsable una certificación sobre los bancos que se encuentren inscritos a su nombre.

Es importante recalcar que cada vez que un organismo público genera un nuevo banco de datos personales, tiene quince días contados desde el inicio de las actividades para proceder a su inscripción. Es responsabilidad del organismo público a cargo del banco de datos personales comunicar cualquier cambio de los elementos que componen la inscripción, pues se presume que la información registrada es verídica y actualizada (art. 22 inc. segundo LPVP). Para estos efectos, también se contempla un plazo de quince días.

Cualquier contravención a las obligaciones indicadas acarreará al menos responsabilidad de carácter administrativo para el funcionario encargado de materializarlas, sin perjuicio de otras que en el caso específico puedan concurrir.

Por otro lado, el Registro Civil está obligado a otorgar por medios electrónicos un informe en el cual conste el nombre de un banco de datos personales, las menciones acerca de la información que contiene y el nombre del organismo público responsable de su registro, a cualquiera que lo solicite.

Por último, para corroborar lo anterior, recomendamos contrastar con la tabla Nº 8 donde aparecen algunos bancos de datos personales del sector salud que deben ser obligatoriamente inscritos ante el Registro Civil según la normativa legal y reglamentaria analizada, correspondiendo a la falta de interoperabilidad su mayor deficiencia.

5.- RÉGIMEN INFRACCIONAL.[16]

A. LA SITUACIÓN NACIONAL.

Un defecto, que a todas luces adolece el marco jurídico de las fichas clínicas, corresponde al disperso régimen sancionatorio de este, que se manifiesta al observar que el principal cuerpo legal sobre la materia —la LDDP—, nada prescribe para los casos en que terceros traten indebidamente a las fichas clínicas, ya sea accediendo, modificando, eliminando o divulgando su contenido.

Así, por ejemplo, la ley simplemente declara que por regla general los terceros no pueden acceder al contenido de las fichas (artículo 13), salvo excepciones legales, pero desatiende el establecimiento de sanciones específicas para el caso de que ello tenga lugar. Lo propio ocurre al tratarse de accesos, rectificaciones, eliminaciones o vulneraciones al deber de secreto, confidencialidad o reserva. Incluso, omite una referencia explícita para algo tan grave como la comercialización de fichas clínicas, que incluso puede llegar a involucrar información personal de NNA.

Por esta razón, frente a las omisiones de la LDDP no queda más que recurrir a las reglas generales sobre sumarios sanitarios, contenidas en el Libro X del Código Sanitario, que se

[16] A modo de complemento, la presente investigación está acompañada de un anexo denominado "Jurisprudencia relevante sobre Fichas Clínicas".

traducen en multas; sin perjuicio de que el artículo 174 inciso 3º también permite la clausura de establecimientos, cancelación de autorización de funcionamiento, decomisos, entre otros. Esto se desprende a partir de lo dispuesto en el artículo 129 letra E del mismo código, que explícitamente establece dicho mecanismo para la determinación de eventuales responsabilidades frente a las infracciones a la ley.

Así las cosas, es menester atender a la persona que comete la infracción, debido a que los regímenes aplicables son distintos según se trate de un funcionario público o de un particular. En el caso de los primeros, además de los sumarios sanitarios, son susceptibles de ser objeto de sumario administrativo por infracción a "obligaciones o deberes funcionarios", según lo establece el artículo 119 del Estatuto Administrativo.

Además, la disposición siguiente expresamente determina que la responsabilidad administrativa "es independiente de la responsabilidad civil y penal", debiendo prevenir al respecto que en ciertos casos dicha declaración pueda reñir con el principio general del derecho relativo al *non bis in ídem*. Esta idea se reitera —en términos distintos— con el artículo 174 inciso final del Código Sanitario con ocasión de los sumarios sanitarios.

Asimismo, la responsabilidad administrativa del funcionario público puede derivarse del incumplimiento de su obligación de "guardar secreto en los asuntos que revistan el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales", según prescribe el artículo 61 letra h) del Estatuto Administrativo.

Sobre el particular cabe acotar que la confidencialidad que amerita el tratamiento de las fichas clínicas está además resguardada por el "secreto estadístico" consagrado en los articulo 29 y 30 de la ley Nº 17.374, que crea el INE.

En efecto, los organismos fiscales, semifiscales y Empresas del Estado, así como cada uno de sus respectivos funcionarios, "no podrán divulgar los hechos que se refieren a personas o entidades determinadas de que hayan tomado conocimiento en el desempeño de sus actividades".

Ahora bien, trasladándonos a sede penal, las únicas normas aplicables son los artículos 246 a 247 bis sobre violación de secretos, que conforman una especial categoría de los delitos funcionarios regulados por el Título Quinto del Libro Segundo del Código Penal.

Por otra parte, respecto de los particulares, no puede llegar a configurarse la responsabilidad administrativa ni menos penal porque carecen de esta especial condición. Naturalmente, lo anterior tiene por efecto que el régimen sancionatorio para los privados sea exiguo —incluso menor que el de los funcionarios públicos— por no existir nada semejante a la tipificación de conductas que sancionen el acceso, divulgación o destrucción ilícita de las fichas clínicas.

Tampoco ayuda el hecho de que nuestra ley de delitos informáticos (Nº 19.223) se encuentre obsoleta, si consideramos que su publicación data del año 1993, época en que internet no era un servicio masivo para la ciudadanía. Además, esta ley de antemano surgió con severas inconveniencias en un aspecto tan central como el bien jurídico protegido, que no resulta fácilmente identificable. Siguiendo a Hernández, si bien el propósito inicial del legislador fue afrontar los desafíos de las nuevas tecnologías, dicha finalidad fue abandonada cuando se optó por hacer aplicables sus disposiciones "en parte también a la afectación del *hardware* y de datos no informáticos", un aspecto "plenamente abarcad[o] por la legislación anterior".[17]

En efecto, el año 1999 —es decir, al poco tiempo de ser publicada—, la doctrina ya alertaba que la ley Nº 19.223 era meritoria, aunque insuficiente para combatir el delito informático.[18] Esto se ve reflejado en la no tipificación del simple acceso a un sistema informático, esto es, la "acción destinada a violar las medidas de seguridad de un ordenador, sin ánimo de apoderarse, usar o conocer la información contenida en este o ánimo de alterar los datos".[19]

Así, por ejemplo, el mero acceso a las bases de datos de fichas clínicas electrónicas almacenadas por un servicio de salud público realizado por un particular, carecería de sanción penal según la legislación vigente, cuestión que no guarda relación con la gravedad de la acción. Las inconveniencias de ello pueden ser peligrosas; por ejemplo, un individuo podría tomar conocimiento del estado de salud de una persona políticamente expuesta y usar dicha información para fines perjudiciales.

Sin perjuicio de lo anterior, debemos atender a lo que esta ley dispone, pues pese a las críticas señaladas, continúan vigentes sus disposiciones referentes al sabotaje y espionaje

[17] HERNÁNDEZ, Héctor. Tratamiento de la criminalidad informática en el derecho penal chileno: Diagnóstico y propuestas. Informe solicitado por la División Jurídica del Ministerio de Justicia, 2001. p. 4.
[18] MAGLIONA, Claudio y LÓPEZ, Macarena. Delincuencia y fraude informático. Editorial Jurídica de Chile, 1999. p. 173-174.
[19] Op. Cit. p. 178.

informático. Siguiendo a Mayer y a Oliver, “el conjunto de delitos informáticos en sentido estricto, esto es, de los comportamientos que afectan el software o soporte lógico de un sistema de tratamiento automatizado de la información, está compuesto por tres ilícitos principales: el sabotaje, el espionaje y el fraude informático”, frente a lo cual debemos advertir que nuestra ley ha optado por prescindir de la tipificación de este último.[20]

Pues bien, una vez aclarado lo anterior, podemos indicar que el sabotaje informático está tipificado en el artículo 1º, el cual sanciona con pena de presidio menor en su grado medio a máximo al que “maliciosamente destruya inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento”, pero si como consecuencia de estas conductas se afectan datos contenidos en el sistema, la pena aumenta a presidio menor en su grado máximo.

Asimismo, está recogido en el artículo 3º referido a quien “maliciosamente altere, dañe o destruya los contenidos en un sistema de tratamiento de información”, conducta sancionada con presidio menor en su grado medio.

El espionaje informático, por su parte, está tipificado en el artículo 2º de la ley, castigando al que “con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él” con pena de presidio menor en su grado mínimo a medio.

No se debe confundir la referida conducta con la revelación o difusión de los datos, pues son figuras distintas y autónomas. El artículo 4º de la ley 19.223 castiga al que “maliciosamente revele o difunda los contenidos en un sistema de información” con pena de presidio menor en su grado medio y en el caso de que el autor sea el responsable del sistema de información, la pena aumenta en un grado.

En consecuencia —siguiendo a Mayer y a Vera—, “[…] mientras que el espionaje informático supone una intromisión, en el sentido de que ha de existir un acceso a y conocimiento indebido de datos de un sistema informático, la revelación o difusión de los datos implica develarlos indebidamente respecto de terceros.”.[21]

---

[20] MAYER, Laura y OLIVER, Guillermo. El delito de fraude informático: concepto y delimitación, Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 1, 2020. p. 154.

[21] MAYER, Laura y VERA, Jaime. El delito de espionaje informático: concepto y delimitación, Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 2, 2020. p. 227.

En todo caso, debemos agregar que la ley no contempla mecanismos especiales para la investigación de los delitos informáticos —tales como los dispuestos en el artículo 226 bis del Código Procesal Penal—, facilitando la impunidad digital. Por ello, estimamos que representaría un avance sustantivo la pronta la publicación del PDL que adecúa nuestra legislación al Convenio de Budapest sobre Ciberdelincuencia.[22] [23]

En nuestro país, tanto funcionarios públicos como particulares tienen en común que además de ser objeto de sumarios sanitarios, también pueden ser civilmente responsables por los daños que causen —incluyendo el monto que se determine por concepto de daño moral—, toda vez que residualmente aplican las reglas generales del Código Civil.

En el ámbito jurisprudencial, encontramos algunos asuntos en que se han referido a las normas antes señaladas. Así, por ejemplo, la Corte de Apelaciones de Santiago ha fallado que constituye negligencia médica y falta de servicio el extravío de fichas clínicas de una paciente que fue dada de alta a pesar de presentar daño hepático, por lo que ha condenado al pago de 25 millones de pesos por daño moral.[24]

La responsabilidad civil también se verifica tratándose de infracciones a la normativa sobre PDP en virtud del artículo 23 LPVP. Por ejemplo, el 24º Civil de Santiago determinó que la divulgación, manipulación y tratamiento ilegal de datos de un paciente —considerados sensibles por referirse a su atención médica—, por parte de funcionarios del prestador genera daño moral en los términos de la ley Nº 20.584 (arts. 12 y 13) y LPVP (arts. 4º, 5º, 9º, 10 y 12), relacionado con el tratamiento y cuidado indebido de datos sensibles y su difusión por personas no autorizadas.[25] A este respecto resultan relevantes las acciones de protección y de *habeas data* que los afectados pueden interponer, por más que no persigan la reparación del mal causado sino más bien el restablecimiento del derecho.

En el caso de las acciones de protección, la Corte Suprema ha sostenido, por ejemplo, que contraviene al ordenamiento jurídico que un establecimiento de salud les exija a los hijos

[22] PDL que “Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest” (boletín 12.192-25).
[23] A saber, el Convenio de Budapest corresponde al principal instrumento internacional para combatir el cibercrimen. La apertura del tratado se remonta al año 2001 y su entrada en vigor al año 2004. A agosto de 2021, posee la adhesión de más de cuarenta países. Recurso en línea disponible en: https://bit.ly/3CbkywP. [consulta: 06 febrero 2022]
[24] SCA Santiago Rol Nº 2.584-2017.
[25] Sentencia 24º Civil de Santiago Rol Nº 20.855-2014.

practicar la posesión efectiva como requisito previo al acceso a la ficha clínica de su fallecido progenitor.[26]

En cambio, en el caso de las acciones de *habeas data*, debemos tener presente que su uso no se encuentra masificado, puesto que no es capaz de competir frente a la celeridad y amplitud que ofrece la acción de protección. Sin perjuicio de lo anterior, la Corte de Apelaciones de Santiago ha fallado, por ejemplo, que un perito está obligado a entregar los resultados de todos los exámenes y pruebas realizadas a una persona con ocasión de una causa tramitada ante los tribunales de familia toda vez que se trata del titular de aquellos datos personales.[27]

Por último, es importante recalcar que la fiscalización del cumplimiento de la ley respecto de organismos públicos que traten fichas clínicas, por regla general es de competencia de la CGR. En esta línea, se ha determinado que no procede la entrega a las municipalidades de datos sensibles de salud relativos al diagnóstico de pacientes COVID-19, sin que exista consentimiento específicamente manifestado para estos efectos o una ley habilitante que lo precise.[28] Asimismo, se ha definido que la autoridad administrativa, en el nivel jerárquico que sea, debe establecer y hacer efectiva la responsabilidad administrativa de los funcionarios que permitieran que las bases de datos que contienen información sensible de los usuarios de los establecimientos de salud, hayan sido transmitidas al personal de unidades que, en razón de sus funciones, no esté habilitado para acceder a las mismas, dado que dicha divulgación no se encuentra permitida por la normativa.[29]

De todos modos, es importante el rol del CPLT, por tratarse de la entidad encargada de fiscalizar el cumplimiento de la normativa relativa a los datos personales por parte de los organismos públicos en conformidad con el artículo 33 (letra m) de la ley Nº 20.285. En efecto, en ejercicio de esta potestad, el CPLT recientemente ha dictado recomendaciones para que los organismos públicos respeten las normas sobre PDP y adopten medidas de seguridad especiales en el contexto del tratamiento de datos sensibles que la pandemia de COVID-19 ha propiciado.[30] De igual modo, con motivo de la pandemia, ha emitido recomendaciones para que las aplicaciones móviles de monitoreo de pacientes contagiados

[26] SCS Nº 32.059-2014.
[27] SCA Santiago Rol Nº 13.251-2019.
[28] CGR Nº 8.113 de 2020.
[29] CGR Nº 52.957 de 2016 (aplica Nº 3.421 de 2016).
[30] CPLT Rol Nº 157/2021.

(*CoronApp)*, las compras y contrataciones de hospitales y servicios de salud, las iniciativas de trazabilidad y de toma de PCR, así como el proceso de vacunación de la población, estén ajustadas a las disposiciones de la LPVP.[31]

Por otro lado, al CPLT —en tanto organismo público encargado de garantizar el derecho de acceso a la información— le ha correspondido conocer amparos que involucran solicitudes de acceso a datos de salud o fichas clínicas. Por ejemplo, ha rechazado un amparo deducido en contra de la Policía de Investigaciones de Chile, interpuesto por la negativa de la institución de hacer entrega de veintidós informes técnicos que otorgaron jubilación por invalidez fundados en la existencia de patologías mentales en funcionarios. En concepto del Consejo, el acceso a los antecedentes importaría un riesgo de divulgación de información de carácter altamente sensible de los titulares, pudiendo afectar su esfera específicamente privada.[32]

Sin embargo, en casos en los que se ha solicitado una amplia cantidad de información —incluyendo datos sensibles—, el CPLT sí ha accedido, pero obligando a que se lleve a cabo un adecuado proceso de anonimización que impida la determinación posterior de la identidad de las personas a través de mecanismos como el cruce de datos con información que circula libremente en internet. En efecto, el año 2016 el Consejo obligó a que la SUPERSALUD hiciera entrega anonimizada de todos los contratos, prestaciones y cotizaciones de salud —entre otros— que esta entidad posee sobre la población, debiendo tarjar o eliminar el RUT y otros datos indicados en cada caso, con el propósito de que la identidad de los titulares se mantenga resguardada.[33]

Por último, es relevante la jurisprudencia que la SUSESO va configurando, pues delimita —en el orden administrativo— la interpretación de las normas legales y reglamentarias de su competencia, lo que concierne en determinadas ocasiones a la regulación de las fichas clínicas.

En este sentido, la SUSESO ha determinado que las mutualidades de empleadores, en su carácter de organismos administradores del Seguro Social de la ley N° 16.744, se encuentran legalmente habilitadas para acceder a la información contenida en las fichas clínicas de los trabajadores de sus empresas adherentes o afiliadas, tanto cuando les

[31] CPLT Roles Nºs 675/2020; 746 y 748/2020; 1155/2020 y 58/2021; 868/2020; 43, 116 y 179/2021 (respectivamente).
[32] CPLT Rol Nº C1.511-21.
[33] CPLT Rol Nº 2.075-16.

brinden atención médica en sus propios centros médicos, como cuando los deriven a sus prestadores médicos en convenio.[34]

RÉGIMEN SANCIONATORIO DE LAS FICHAS CLÍNICAS					
	SUMARIOS SANITARIOS	**RESP. ADM.**	**RESP. ADM. (PDP)**	**RESP. CIVIL**[35]	**RESP. PENAL**[36]
PARTICULARES	Sí	No	No	Sí	No
FUNCIONARIOS PÚBLICOS	Sí	Sí	Sí	Sí	Sí (solo en relación con deber confidencialidad por arts. 246 a 247 bis Código Penal)
PJ PRIVADO	Sí	No	No	Sí	No
PJ Dº PÚBLICO	No	No	CPLT tiene competencia respecto de ellos, pero no existe un catálogo claro de infracciones. Por ello, se remite a hacer recomendación-es. CGR también fiscaliza y vela por el cumplimiento de la ley.	Sí	No

TABLA 2. ELABORACIÓN PROPIA.

B. LA SITUACIÓN DE DERECHO COMPARADO.

La tenue respuesta penal de nuestra legislación contrasta con aquellas que otras jurisdicciones contemplan para conductas ilícitas relativas a las fichas clínicas. De ello se desprende que el caso de Chile constituye una anomalía.

Por ejemplo, en EE.UU., la *Health Insurance Portability and Accountability Act* establece penas severas por la divulgación de los "datos identificatorios del paciente" (*personal health*

[34] SUSESO Rol Nº 45.512-2018.

[35] A pesar de que siempre es procedente, su gran desventaja consiste en la excesiva dilación, afectando el sentido de justicia del recurrente.

[36] Cabe prevenir que, aunque existe la ley de delitos informáticos, esta no tipifica conductas que se refieran exclusivamente a las fichas clínicas, razón por la cual la hemos excluido de la presente tabla.

information). En este sentido, la pena por vender transferir o utilizar datos de salud para beneficio comercial puede llegar a los $250.000 dólares y 10 años de cárcel.[37]

De modo similar, en Australia el uso inapropiado o desautorizado de las fichas clínicas está sancionado con hasta cinco años de cárcel y/o multas de hasta $333.000 dólares para personas naturales y $1.665.000 dólares para las jurídicas.[38]

Asimismo, en Canadá los delitos que involucran el tratamiento ilícito de fichas clínicas o datos de salud están sancionados con hasta un año de cárcel y/o multas con un máximo de $200.000 dólares para las personas naturales y $1.000.000 para las jurídicas.[39]

Mientras tanto, entre los países de la UE sobresale el caso de España, pues lejos de contemplar figuras penales específicas para las fichas clínicas, opta por una remisión al régimen general contenido en el Código Penal. En efecto, al abordar los delitos relativos al descubrimiento o revelación de secretos (artículos 197 a 201), sanciona con una pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses a quien, careciendo de autorización y en perjuicio de terceros, se apodere, utilice o modifique datos personales en soporte electrónico. También v. gr. sanciona con una pena de dos a cinco años a quien ceda a un tercero los datos personales obtenidos ilícitamente. Adicionalmente, se prevén infracciones y sanciones por incumplimiento de la normativa de protección de datos, conforme a los artículos 70 y siguientes de la ley de protección de datos personales.

Finalmente, en el caso europeo debemos destacar las sanciones complementarias previstas en el RGPD, en su artículo 84.2.

6.- OTROS CUERPOS NORMATIVOS COMPLEMENTARIOS A LA REGULACIÓN DE LA FICHA CLÍNICA.

Entre aquellos cuerpos legales, reglamentarios o de *soft law* complementarios a la regulación de la ficha clínica podemos mencionar:

a. La reciente ley Nº 21.331, sobre reconocimiento y protección de las personas en la atención de salud mental: por cuanto contempla la obligación de dejar constancia

[37] Recurso en línea: *Summary of the HIPAA Privacy Rule*, p. 18. Disponible en: https://bit.ly/3fstynA. [consulta: 06 febrero 2022]
[38] *My Health Records Amendment (Strengthening Privacy) Bill 2018*, *División 3A—Offences and penalties in relation to use of My Health Record-derived information for prohibited purpose*.
[39] *Personal Health Information Protection Act, Section 72.*

en la ficha clínica cuando la persona esté impedida de consentir sobre una determinada acción de salud (art. 4). En un sentido similar, respecto al deber de dejar constancia en la ficha clínica de todas las medidas de contención para el manejo de conductas perturbadoras o agresivas (art. 21).

b. Ley Nº 21.067, que "crea la Defensoría de los Derechos de la Niñez": en cuanto, como hemos indicado anteriormente, sus artículos 4º letras b) y e), 8º y 16, otorgan legitimación activa a esta institución para acceder a las fichas clínicas de NNA tanto para velar por sus derechos como para perseguir a terceros a consecuencia de ello.
c. Ley Nº 21.258, que crea la Ley Nacional de Cáncer, que rinde homenaje póstumo al doctor Claudio Mora: en cuanto al regular en el artículo 8º el Registro Nacional del Cáncer, indica que esta enfermedad es de notificación obligatoria y ello tiene por consecuencia que las fichas clínicas deban interoperar con el registro que eventualmente se vaya a implementar.
d. Ley Nº 20.405 del INDH: con el objeto de resolver adecuadamente cuestiones que pertenezcan al ámbito de su competencia, el Consejo puede requerir información y antecedentes a otras entidades que formen parte de la Administración del Estado (artículo 8º numeral 6º). Debido a la amplia técnica legislativa empleada, quedan incluidas las fichas clínicas.
e. Ley 20.379: que crea el sistema intersectorial de protección social e institucionaliza el subsistema de protección integral a la infancia "Chile crece contigo" que entrega al Ministerio de Planificación (hoy MIDESOFA) la administración, coordinación, supervisión y evaluación de la implementación del Sistema. El mismo cobra relevancia porque consiste en un sistema integral de apoyo a los NNA desde su gestación hasta la adultez, incluyendo la atención de salud.
f. FOS: es importante notar que la autoridad sanitaria al solicitar el auxilio de la fuerza pública (artículos 8º y 155 del Código Sanitario) puede configurar situaciones en las que los miembros de las FOS accedan a fichas clínicas. Ello, a pesar de que las leyes orgánicas de Carabineros de Chile y de la Policía de Investigaciones no los habilite específicamente.
g. DFL Nº 251 sobre Compañías de Seguros, Sociedades Anónimas y Bolsas de Comercio: por cuanto habilita, en el artículo 61, a los liquidadores de siniestros para acceder a información contenida en las fichas clínicas de pacientes que digan directa relación con la ocurrencia de un siniestro. La norma precisa que el acceso

por los liquidadores no es amplio, sino que el Ministerio Público u otras autoridades administrativas deben certificar los puntos necesarios para practicar la liquidación.

h. Ley Nº 16.395: en cuanto establece que la SUSESO, en el cumplimiento de sus funciones, puede requerir acceso a los sistemas de información de las instituciones fiscalizadas (arts. 2 letra g) y 35).
i. Ley Nº 16.744: al igual que el caso anterior, autoriza al Instituto de Seguridad Laboral, Mutualidades de Empleadores y Servicios de Salud a acceder a fichas clínicas en el cumplimiento de sus funciones.
j. Código de Ética del Colegio Médico: contiene un capítulo completo dedicado a la regulación del secreto profesional (artículos 29 a 38), en el que sobresale la prohibición de los médicos para participar en la constitución de bancos de datos sanitarios en los que la reserva de confidencialidad no esté garantizada (art. 35).
k. Oficio Circular Nº 7 de la Intendencia de Prestadores de Salud (IP) sobre Telemedicina de abril de 2020: este oficio dictado a propósito de la pandemia de COVID-19 permite que "[…] las consultas de seguimiento y/o control, se pueden hacer en forma remota, siempre y cuando el profesional conozca o tenga acceso al historial clínico del paciente, debiendo efectuarse dicho acceso de forma controlada […]". "[…] **las personas que tendrán acceso a la ficha clínica de sus pacientes**, **serán registrados previamente por el prestador**, en la respectiva ficha clínica, […] **quien deberá determinar a quiénes y cuando entrega la autorización para acceder a la información clínica que se solicita**, circunstancia que **además debe ser informada al paciente antes der inicio de la prestación**, a fin de que **conozca que se accederá a su ficha**, **en qué circunstancias** y **para qué efectos**, lo que se presumirá por éste, por el hecho de acceder a la ejecución de esa prestación remota" (el destacado es nuestro).
l. Proyecto de Resolución de la Cámara de Diputados de fecha 19 de junio de 2018: a través del cual se le solicitó al presidente de la república el patrocinio de un PDL que establezca un sistema integrado de ficha clínica electrónica universal de pacientes del sector público y del sector privado.

7.- SÍNTESIS DEL CAPÍTULO I.

Hasta el momento hemos abordado integralmente el marco jurídico de las fichas clínicas en sus diferentes formas normativas. Dicho análisis comienza con la identificación del derecho a la salud y la protección de los datos personales como los derechos

fundamentales sobre los que se erige el marco general de nuestro objeto de estudio: la interoperabilidad de las fichas clínicas.

En primer lugar, hemos advertido que, si bien la Constitución consagra el derecho a la salud y a la protección de datos personales, no se detalla la regulación del acceso a la información de salud para concretar esta garantía, como uno de los objetivos prioritarios de la labor que se atribuye al Ministerio de Salud. Lo mismo advertimos a nivel legal, en que no se explicita las normas que permitan garantizar el acceso oportuno a esta información por parte de los profesionales que participan directamente de las acciones de promoción, protección y recuperación de la salud de la persona.

Sin embargo, consideramos que concordando los numerales del artículo 19 con las normas de las bases de la institucionalidad, especialmente en lo que se refiere al principio de coordinación— sí es posible derivar la existencia jurídica de la interoperabilidad de las fichas clínicas, así como el correlativo deber del Estado de garantizarla.

Estimamos que se trata, en definitiva, de que el Estado, con ayuda de la tecnología, consiga optimizar la forma en que materializa su deber de supervigilar las acciones relacionadas con la salud, pudiendo mejorar las condiciones de bienestar que en la actualidad es capaz de ofrecer a la población.

Esto se sustenta en diversos pronunciamientos jurisprudenciales que han ido paulatinamente recalcando la importancia de que el Estado cumpla las directrices que impone el principio constitucional de coordinación. De esta manera, en relación con las fichas clínicas, sería posible obtener un "[…] cumplimiento más eficiente y eficaz de la función administrativa y la mayor satisfacción de las necesidades colectivas a cargo del Estado, con el menor costo financiero y social posible".[40]

Por otra parte, hemos definido y caracterizado el marco legal aplicable a las fichas clínicas —compuesto primordialmente por las LDDP y LPVP—, observando que tampoco existe alusión alguna de la interoperabilidad. Ello, sin duda, contrasta con iniciativas comparadas que incluso pretenden extender esta cualidad hacia toda la Administración del Estado, como la Ley Marco de Interoperabilidad de la UE o el programa *eHealth* de la CE.[41]

[40] SCS Rol Nº 34.536-2017, considerando 7º.
[41] Recurso en línea: Salud en línea (*eHealth*). Disponible en: https://bit.ly/3BU6TZD. [consulta: 06 febrero 2022]

Quizás el intento que más se aproxima es la definición de ficha clínica contenida en el artículo 12 de LDDP, al reconocer que este instrumento "tiene como finalidad la integración de la información necesaria en el proceso asistencial". Advertimos, en todo caso, una brecha reglamentaria, pues el Decreto Nº 41 —especialmente el artículo 8, que establece los requisitos de las fichas en soporte electrónico— desperdicia la oportunidad de regular la integración de la información de salud que sí está digitalizada. Por lo tanto, un esfuerzo reglamentario permitiría dar mayor fuerza a estos imperativos, además de contribuir a la seguridad y certeza jurídica.

Además, debemos añadir otras deficiencias del marco legal y reglamentario que impiden generar un nivel de protección suficiente para las personas, o que al menos mitigue los riesgos asociados. Es el caso del débil y difuso régimen infraccional previsto para repeler y castigar las manipulaciones o tratamientos de fichas clínicas que sean contrarias a la ley, con especial énfasis en que no existe una respuesta penal semejante a la considerada en otras latitudes como EE.UU., Australia, Canadá y España. Sobretodo considerando que Chile aún no termina de adecuar su legislación a las prerrogativas del Convenio de Budapest sobre Ciberseguridad.[42]

En al ámbito institucional, la inexistencia de una autoridad de control del tratamiento de datos personales independiente y empoderada que tenga potestades suficientes sobre personas naturales y jurídicas, tanto públicas como privadas genera que no exista la capacidad institucional y técnica para fiscalizar el debido tratamiento de las fichas clínicas en tanto son datos personales de carácter sensible. Así, la autoridad carece de las herramientas idóneas para, por ejemplo, tomar conocimiento de transacciones comerciales de fichas clínicas y sancionarlas oportunamente.

Frente a esta precariedad regulatoria, confluyen diversos actores, tales como los tribunales de justicia, MINSAL, CPLT, CGR o SUSESO cuya jurisprudencia ha ido supliendo las deficiencias y omisiones antes señaladas. Sin embargo, cada procedimiento atiende a objetos distintos y en ningún caso es capaz de reemplazar la labor de las entidades dotadas de las competencias necesarias para implementar la interoperabilidad de las fichas clínicas.

[42] PDL que "Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest" (boletín 12.192-25).

CAPÍTULO II. LA INTEROPERABILIDAD DE LA FICHA CLÍNICA.

1.- ¿QUÉ ES LA INTEROPERABILIDAD?[43]

Un primer acercamiento al concepto de interoperabilidad lo ofrece la definición de la Organización Mundial de la Salud (OMS), que concibe a la interoperabilidad como "la capacidad de distintas aplicaciones de acceder, intercambiar, integrar y usar datos de forma colaborativa y coordinada mediante la utilización de interfaces y estándares comunes, dentro o fuera de un mismo ámbito institucional, regional y nacional, para proporcionar una portabilidad rápida y fluida de la información y optimizar los resultados sanitarios".[44]

Sin embargo, la definición ampliamente utilizada a nivel global, tanto por académicos como por organizaciones, corresponde a la del IEEE, que considera a la interoperabilidad como "la habilidad o capacidad de dos o más sistemas de intercambiar información y utilizar la información intercambiada".[45]

En términos sucintos, el BID ha definido a la interoperabilidad como la "**habilidad de intercambiar datos sin errores, interpretar los datos y hacer un uso eficaz de los datos intercambiados**".[46]

En este trabajo nos guiaremos por esta última definición.

Ahora bien, para referirnos al ecosistema de salud digital interoperable nacional, siguiendo a la OMS, adoptaremos la siguiente definición: "todo tipo de infraestructuras informáticas digitales establecidas a nivel nacional en un país que son de carácter interoperable y cuyos principales usuarios son la comunidad en salud, en particular los proveedores de servicios de salud, el personal sanitario y los pacientes, así como las autoridades de salud pública y las instituciones académicas y de investigación. Permiten el intercambio y el tratamiento de

---

[43] Recurso en línea: Introducción a la Interoperabilidad en Salud CTD Corfo. Disponible en: https://bit.ly/3kgsGEM. [consulta: 06 febrero 2022]

[44] OMS. Estrategia mundial sobre salud digital 2020-2025, 2021. p.48.
Esta definición es congruente con la impulsada por la *Healthcare Information and Management Systems Society*, una ONG ampliamente reconocida en el uso de TIC en el ámbito de la salud. Recurso en línea disponible en: https://bit.ly/3wuCHDb. [consulta: 06 febrero 2022]

[45] BID. Interoperabilidad para principiantes: la base de la salud digital. 2019. p. 7.
La PAHO también usa esta definición, por ejemplo, el año 2016 en el estudio "Revisión de estándares de interoperabilidad eSalud en Latinoamérica y el Caribe".

[46] BID. Transformación digital del sector salud en América Latino y el Caribe: La historia clínica electrónica, 2019. p. 13.

datos sanitarios que suelen generar principalmente los proveedores de servicios de salud entre sí y la comunidad en salud".[47]

2.- CRONOLOGÍA DE LA INTEROPERABILIDAD EN LA ADMINISTRACIÓN DEL ESTADO.

La interoperabilidad es un concepto que fue introducido hace bastantes años en nuestra legislación y cuyo primer antecedente se remonta al año 1999, cuando fue promulgado por el Presidente de la República el "Acuerdo marco de cooperación destinado a preparar, como objetivo final, una asociación de carácter político y económico entre la Comunidad Europea y sus Estados Miembros, por una parte, y la República de Chile, por otra parte", a través del Decreto Nº 213 del Ministerio de Relaciones Exteriores, de 1999. Lo anterior, sin perjuicio de que el precitado acuerdo fue suscrito el año 1996 y aprobado por el Congreso Nacional al año siguiente.

En específico, el número 2º letra f) del artículo 19, que trata sobre "la cooperación en el sector de la sociedad de la información y de las telecomunicaciones", dispone que: "2. Las medidas de cooperación en este sector se orientarán en particular hacia: f) la interconexión y la interoperabilidad entre redes y servicios telemáticos comunitarios y chilenos".

Posteriormente, el año 2002, se menciona la interoperabilidad en el Decreto Nº 181 del MINECON, que "Aprueba reglamento de la ley Nº 19.799 de 2002, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma". Sin embargo, este decreto no desarrolló el concepto ni formuló lineamientos asociados a su concreción.

No obstante, más allá de sus omisiones, el decreto sobresale por haber creado el Comité de Normas para el Documento Electrónico, cuya labor dará pie para que, el año 2004, se dicte el Decreto Nº 81 de 2004 SEGPRES, a través del cual se "Aprueba norma técnica para los órganos de la Administración del Estado sobre interoperabilidad de los documentos electrónicos", el cual estuvo vigente hasta el 27 de febrero de 2014, en que fue derogado por el Decreto N° 14 del Ministerio Secretaría General de la Presidencia.

Pues bien, los objetivos planteados por el Comité fueron la interoperabilidad de los documentos electrónicos entre diferentes plataformas, a nivel de hardware, software y sistemas operativos; facilitar tanto la clasificación, almacenamiento y búsqueda de documentos electrónicos como el desarrollo de aplicaciones genéricas para procesar

[47] OMS. Estrategia mundial sobre salud digital 2020-2025, 2020. p. 49.

documentos electrónicos; simplificar el acceso a la información que posee el Estado; aumentar la productividad y reducir los costos operacionales de los órganos de la Administración del Estado; y, por último, facilitar, mediante el uso de TIC, la relación de la ciudadanía y el sector privado con los órganos de la Administración del Estado, así como las interacciones que se produzcan entre los distintos organismos que la componen.

En ese entendido, el decreto definía, en el artículo 5º, una serie de conceptos, incluyendo el de interoperabilidad, con el objeto de uniformar el significado técnico de cada uno y evitar malentendidos cuando estos términos fueran empleados por la Administración del Estado. Es así como define interoperabilidad como la "capacidad que permite a sistemas heterogéneos, operar y comunicarse entre sí". Adicionalmente, concibe a la interoperabilidad como un requisito general que deben satisfacer todos los documentos en formato digital. De esta manera, los documentos electrónicos se caracterizan por ser flexibles, extensibles y permanentes en el tiempo; estar dotados de un sistema multiplataforma; y, además, por ser interoperables.

Por último, el decreto cierra con la habilitación que el artículo quinto hace al Comité para iniciar de oficio o a petición de parte un procedimiento de normalización con sugerencias al presidente de la república donde sean considerados los planteamientos del sector público, privado y de las universidades, con el objeto de que velar por la actualización permanente de estas normas.

Pese a las bondades de la norma, la experiencia del Comité no fue satisfactoria, cuestión que es recogida en el considerando 5º del decreto Nº 14, de 2014, de MINECON en los siguientes términos: "durante los años [el Comité de Normas para el Documento Electrónico creado por el decreto supremo Nº 181] ha mostrado no poder cumplir con dicha función dado que, en su calidad de comité ad hoc, solo funciona de forma esporádica".

Como consecuencia de lo anterior, el año 2014 se modifica el decreto Nº 181 para otorgarle a la SEGPRES —en su calidad de ministerio encargado de la función de coordinar la gestión del gobierno— la facultad de fijar normas técnicas.[48] Esta habilitación se realiza, además, sobre la base de que a esta cartera de Estado le corresponde el desarrollo e implementación del Gobierno Electrónico.

[48] Considerandos 6º y 7º del decreto Nº 14 de MINECON.

Asimismo, para cumplir este cometido, el decreto Nº 14 permite a la SEGPRES adoptar los estándares internacionales emitidos por organismos reconocidos en la materia, aspecto que resulta trascendental para el objeto de la presente investigación. En efecto, únicamente a falta de dichos estándares, puede considerar a los de carácter regional y, solo de modo residual, puede observar los de desarrollo nacional.

Ahora bien, cabe mencionar que a esta reforma al decreto Nº 181 le precedió la realizada el año 2012 mediante el decreto Nº 154 del MINECON, que dotó a este ministerio de las mismas facultades que luego —el año 2014— le serían traspasadas a la SEGPRES. Allí además se establecerían estándares transitorios de certificación, pero omitiendo —lamentablemente— un pronunciamiento acerca de los relativos a la interoperabilidad. Con ello, sin duda, se desperdició una gran oportunidad.

En definitiva, todo el bloque normativo relativo a la interoperabilidad fue sucedido por otros cuerpos legales contemporáneos para lograr profundizar y extender la obligación del Estado de implementar sistemas interoperables en rubros diversos. Muestra de ello es la ley Nº 21.180 de 2019, sobre Transformación Digital del Estado, cuyas enmiendas a la ley Nº 19.880, sobre procedimientos administrativos, resaltan especialmente en cuanto añadieron la interoperabilidad y cooperación como principios de carácter general aplicables a la tramitación por medios electrónicos.

Así las cosas, en virtud del principio de interoperabilidad, los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado, mediante estándares abiertos que permitan una segura y expedita interconexión entre ellos.[49] En cambio, de conformidad con el principio de cooperación, los distintos órganos de la Administración del Estado deben colaborar efectivamente entre sí en la utilización de medios electrónicos.[50]

Incluso, el 11 diciembre de 2021 se publicó su reglamento, el cual regula especialmente la interoperabilidad en el Título VII y, asimismo, el artículo 57 habilita a la SEGPRES para emitir una norma técnica de interoperabilidad para los órganos de la Administración del Estado. Corresponde sin duda a la innovación más importante en esta materia.

[49] Art. 16 bis inciso sexto de la ley Nº 19.880, en su versión modificada por la ley Nº 21.180.
[50] Op. Cit. inciso final.

A mayor abundamiento, otras leyes recientes que han establecido la obligación del Estado de desarrollar y mantener sistemas interoperables son: la ley Nº 20.886 de 2015, que modifica el Código de Procedimiento Civil para establecer la tramitación digital de los procedimientos digitales (artículo 2º letras e) y f)); el Decreto Nº 1930 del Ministerio del Interior por el cual se modifica el Reglamento de Extranjería de modo que la Policía de Investigaciones, Carabineros de Chile y la Autoridad Marítima correspondiente establezcan sistemas de consulta interoperables sobre los registros de entrada y salida de extranjeros; la Nº 20.880 de 2016, sobre probidad en la función pública y prevención de los conflictos de intereses (artículo 6º); la Nº 21.040 de 2017, que crea el sistema de educación pública (artículo 61); la Nº 21.302 de 2021, que crea el Servicio Nacional de Protección Especializada a la Niñez y Adolescencia y modifica las normas legales que indica (artículo 31); y, la Nº 21.305 de 2021, sobre eficiencia energética (artículo 6º).

No obstante, estos esfuerzos, a Chile todavía le pesa la inexistencia de una legislación marco sobre interoperabilidad que regule, en términos globales, esta materia en aquellos espacios que son de competencia del Estado, tal como existe en la UE, incluyendo el ámbito de las fichas clínicas.[51]

Adicionalmente, es deseable desarrollar instrumentos que sean capaces de medir, en términos cuantitativos y cualitativos, el nivel de madurez de interoperabilidad presente en las distintas áreas, de manera tal que la autoridad pueda poner acento en aquellos rubros en los que flaquea, para tener las herramientas que le permitan distinguir entre casos de éxito y fracaso. De esta manera, a vía ejemplar, quienes toman las decisiones podrían ser capaces de comparar los niveles de interoperabilidad en energía versus transportes, o bien evaluar los distintos niveles existentes dentro de un rubro específico.

3.- NIVELES DE INTEROPERABILIDAD.

Ahora bien, no existe una receta para obtener los resultados de la interoperabilidad, sino que se trata de un proceso que tiene distintas variables y, por ello, la academia se ha encargado de distinguirla en varios niveles.

[51] EIF, 2017.

Para estos efectos, existen dos tipos de niveles que permiten acceder hacia miradas diferentes de una misma interoperabilidad. En este sentido, el primero abarca el nivel macro, esto es, desde el punto de la Administración del Estado en todas sus dimensiones[52]:

	NIVEL	DESCRIPCIÓN
En cualquier caso, es necesario determinar un lenguaje homogéneo o común para que la información circule	***Intra-Administrativo***	Cuando existe interoperabilidad entre diferentes agencias o departamentos dentro de una misma unidad administrativa.
	Horizontal	Cuando existe interoperabilidad entre diferentes administraciones en un mismo nivel de gobierno.
	Vertical	Cuando existe interoperabilidad entre diferentes niveles de gobierno dentro de un país
	Regional o Transfronteriza	Cuando existe interoperabilidad entre distintas administraciones, generalmente centrales o a nivel nacional, de diferentes países.

TABLA 3. ELABORACIÓN PROPIA, EN BASE A CRIADO ET. AL. (2011)

En efecto, existe un interés público preponderante en que la interoperabilidad pueda expandirse a todas las áreas que cubre el Estado; el mejor reflejo de esto son los prematuros intentos que la CE ha impulsado desde el 1999 para que ello sea realidad.[53] Lógicamente, este esfuerzo se enmarca en uno mayor, que corresponde a la digitalización de las administraciones públicas, que busca "ahorrar tiempo, reducir costes, aumentar la transparencia y mejorar la calidad de los datos y la prestación de servicios públicos" y, en definitiva, de la transformación digital tanto del aparataje estatal como comunitario.[54]

En este sentido, para el Estado de Chile y sus *stakeholders,* resulta imprescindible contar con información de calidad y oportuna para conseguir un desempeño más eficiente, efectivo y eficaz. A modo de ejemplo, un caso de interoperabilidad a nivel intra-administrativo sería la circulación interna de la información dentro de un mismo Ministerio, respetando, por cierto, las normas sobre PDP. Así, la Subsecretaría de Salud Pública puede requerir, en el ámbito de sus competencias, acceder, en tiempo real, a la información actualizada de que disponga la Subsecretaría de Redes Asistenciales, y esta entidad, a su vez, puede requerir información a un determinado hospital público perteneciente a la Red integrada de Salud, lo cual sería factible si los sistemas se encontraran interconectados y fueran interoperables.

[52] CRIADO, J. Ignacio, GASCÓ, Mila, JIMÉNEZ, Carlos. Interoperabilidad de Gobierno electrónico en Iberoamérica. Estudio comparativo y recomendaciones de futuro. Revista del CLAD Reforma y Democracia, Núm. 50, 2011. p. 3.
[53] EIF, 2017.
[54] Op. Cit.

Un ejemplo a nivel horizontal, en cambio, estaría constituido por el caso en que el Ministerio de Desarrollo Social o de Hacienda requieran de información generada por la Subsecretaría de Salud Pública, como en el caso de "Chile crece contigo", al que nos referimos antes.

A nivel vertical, se consideraría el caso de que el MINSAL solicitara información en tiempo real a una institución de la Red Integrada de Salud o viceversa. O bien que desde la Presidencia de la República se requieran antecedentes a cargo de la SEREMI del Deporte de la Región de Aysén.

En el ámbito regional tomaríamos el mismo ejemplo anterior, pero referido a un CESFAM radicado fuera de la Región Metropolitana, mientras que a nivel transfronterizo correspondería a la información que podría ser compartida entre MINSAL con el de otros gobiernos, o bien con organizaciones internacionales, tales como el la OPS, OMS, OCDE, BID u otra.

De todas formas, es necesario que ciertos aspectos estén estandarizados para que la información pueda fluir o circular sin obstáculos en la Administración del Estado, lo que se relaciona con el siguiente nivel, centrado en el aspecto micro. Por ejemplo, para atender a estos fines resultan cruciales los requerimientos técnicos, el formato utilizado, el significado del mensaje, así como la resiliencia de los sistemas y cultura organizacional de manera que los sistemas conversen de la mejor manera posible.

En efecto, un nivel distinto lo representan aquellos requerimientos aplicables para evaluar la interoperabilidad específicamente en el rubro de salud, tradicionalmente clasificados por Walker, *Healthcare Information and Management Systems Society (HIMSS),* y *Health Leven Seven*.[55] Sin embargo, debido a la superposición de contenidos que esta variedad produce es que la *European Telecommunication Standards Institute (ETSI*) los ha sistematizado de la siguiente manera:

> **a.- Interoperabilidad Técnica**: vinculada a componentes de *hardware* y/o *software*, sistemas y plataformas que permiten la comunicación que tendrá lugar de máquina a máquina.[56] Cubre las cuestiones técnicas (hardware, software, telecomunicaciones) necesarias para interconectar sistemas computacionales y servicios, incluyendo aspectos clave como interfaces abiertas, servicios de interconexión, integración de

[55] BID. Interoperabilidad para principiantes: La base de la salud digital, 2019. p. 8-9.
[56] PAHO. Revisión de estándares de interoperabilidad para la eSalud en Latinoamérica y el Caribe, PAHO y Oficina Regional para las Américas de la OMS, Washington, D.C., EE.UU., 2016. p. 17.

datos y *middleware*, presentación e intercambio de datos, accesibilidad y servicios de seguridad.[57] Se centra en mover datos desde los sistemas de A hacia B. Esto se grafica en la necesidad de que todos los computadores utilicen un mismo sistema operativo, o que al menos estos sean compatibles (por ejemplo, Microsoft y Apple), puesto que de lo contrario nada podrán comunicar.

b.- Interoperabilidad Sintáctica: relacionada con el formato de los datos intercambiados.[58] Los mensajes, documentos y servicios que se consumen necesitan tener una sintaxis y una codificación bien definidas para que puedan ser interpretados por el software que los recibe.[59] Se trata de que los sistemas A y B cuenten con formatos que hagan interoperables los datos compartidos entre ellos. Por ejemplo, si se trata de fotos, que todas sean en formato JPG o si se trata de documentos escritos, que estos sean en formato Word. La consecuencia práctica de que esto no se implemente correctamente es que la interoperabilidad sintáctica simplemente no tiene lugar o se dilata innecesariamente, por ejemplo, malgastando tiempo en transformar el formato de los archivos.

c.- Interoperabilidad Semántica: vinculada con la interpretación humana del contenido intercambiado, es decir, lo relevante en esta clase de interoperabilidad es el significado. Implica que hay un entendimiento común entre personas sobre el significado del contenido (información) que se intercambia (se garantiza la correcta interpretación y uso de la información intercambiada, para lo cual se necesitan definiciones formales de cada entidad, atributo, relación, restricción y término intercambiado).[60] Se trata de que los datos contenidos en los sistemas A y B sean entendidos de modo unívoco. En este sentido, al compartir información es necesario que tanto significado como significante —siguiendo a Ferdinand de Saussure— sean estandarizados para que, tanto intervinientes como los distintos sistemas informáticos, atiendan un fin equivalente y compartido al tratar la información. Así, por ejemplo, puede ser que el concepto “patología” no sea unívoco para todos los funcionarios que se desempeñan en el MINSAL y las respectivas entidades que dependen de esta cartera de Estado, lo que evidentemente puede traer consecuencias indeseadas una

[57] CEPAL. Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe, 2007. p. 13.

[58] PAHO. Revisión de estándares de interoperabilidad para la eSalud en Latinoamérica y el Caribe, PAHO y Oficina Regional para las Américas de la OMS, Washington, D.C., EE.UU., 2016. p. 17.

[59] BID. Interoperabilidad para principiantes: La base de la salud digital, 2019. p. 9.

[60] PAHO. Revisión de estándares de interoperabilidad para la eSalud en Latinoamérica y el Caribe, PAHO y Oficina Regional para las Américas de la OMS, Washington, D.C., EE.UU., 2016. p. 17.

vez que la información interopere. Más aún, cuando en el sistema de salud existen profesionales de distintas nacionalidades. Por ejemplo, resulta probable que un médico chileno, cubano y venezolano no tengan uniformidad en los conceptos que utilizan periódicamente, lo cual puede dificultar su desempeño e incluso ser potencialmente riesgoso para los pacientes.

d.- Interoperabilidad Organizacional: capacidad de las organizaciones para comunicar y transferir efectivamente los datos, a pesar de que se estén usando una variedad de sistemas de información sobre diferentes infraestructuras, a través de distintas regiones geográficas y culturas, sin perjuicio de que dicho fenómeno en Chile no sea tan acentuado.[61] El obstáculo de este nivel es que para que sea fructífero resulta imprescindible que los otros niveles también lo sean, porque la interoperabilidad organizacional no es más que el resultado de la correcta implementación de los niveles anteriores y, en consecuencia, solo se verificará una vez que se integren todos los datos intercambiados. Se trata, entonces, de que todos los sistemas —más allá de A y B— estén dotados de interoperabilidad para que toda la información pueda circular y estar disponible cuando se le requiera. Por ejemplo, el desafío del MINSAL sería que toda la información con la que está vinculado pudiere interoperar sin que la multiplicidad de sistemas informáticos que procesan información de diferente índole generada a lo largo y ancho del país sea un obstáculo.

Habiendo expuesto la problemática de la que se preocupan los niveles de interoperabilidad para el sector salud, es menester clarificar que existen estándares reconocidos internacionalmente que buscan resolver los inconvenientes que puedan surgir y que se relacionen con aspectos técnicos, sintácticos, semánticos u organizacionales. No obstante, ello será abordado debidamente en su oportunidad, una vez que otros contenidos previos sean analizados.

Cabe prevenir que a nivel comparado se tiende a incluir la interoperabilidad legal o jurídica como un nivel distinto. Ello puede apuntar a la necesidad de homogeneizar la normativa habida al dar cuenta de la existencia de transferencias transfronterizas de datos personales entre países de tradiciones jurídicas diversas como ocurre, por ejemplo, en la comunidad europea. De ahí que el EIF se refiera a la Interoperabilidad Jurídica como aquella que permite “garantizar que las organizaciones que operan con arreglo a diferentes marcos

[61] Op. Cit.

jurídicos, políticas y estrategias puedan trabajar juntas".[62] Sin embargo, este nivel de interoperabilidad puede estar dirigido además, a la necesidad de constituir un marco normativo legal que permita el intercambio de datos y servicios localizados en un mismo país, pero entre instituciones del el sector público con aquellas que pertenecen al sector privado, tanto a nivel horizontal como vertical. Este es el caso de Uruguay.[63]

Ahora bien, debido a que la realidad europea no es aplicable a Chile y que el sentido en que la interoperabilidad legal está empleado por Uruguay es factible de incluir dentro de la interoperabilidad organizacional, emplearemos la clasificación tradicional del ETSI. Además, estimamos que la importancia de segmentar los niveles consiste en la diferenciación de los estándares aplicables para cada cual, cuestión que no ocurre con el nivel legal o jurídico.

4.- FUNCIONES DE LAS FCE SEGÚN EL *INSTITUTE OF MEDICINE.*[64]

Un requisito indispensable para que las fichas clínicas sean interoperables es que estén registradas en soporte electrónico, lo que constituye una cualidad que conlleva una serie de beneficios:

F1.- Almacenamiento y recuperación de información y datos sobre la salud: capacidad para almacenar y recuperar diagnósticos de pacientes, alergias, resultados de laboratorios, medicación, etc.

F2.- Gestión de resultados: capacidad de que todos los proveedores evalúen y utilicen la información sobre pacientes nuevos y antiguos desde diferentes entornos para mejorar los procesos y estrategias de la atención de la salud.

F3.- Entrada y gestión de pedidos: capacidad de introducir y almacenar recetas médicas, análisis y otros servicios para favorecer la legibilidad, reducir las duplicaciones y mejorar la velocidad de gestión de los pedidos.

F4.- Apoyo a la toma de decisiones: capacidad de usar recordatorios, mensajes, alertas y sistemas computarizados de apoyo a la toma de decisiones para mejorar el

[62] EIF, 2017. p. 26.

[63] Recurso en línea: Niveles de interoperabilidad AGESIC. Disponible en: https://bit.ly/3CZvRZ5. [consulta: 06 febrero 2022]

[64] Institute of Medicine. 2003. Key Capabilities of an Electronic Health Record System: Letter Report. Washington, DC, EE.UU.: National Academies Press. EN: BID. Sistemas de Historias Clínicas Electrónicas: Definiciones, evidencias y recomendaciones prácticas para América Latina y el Caribe, 2020. p.13.

cumplimiento de las mejores prácticas clínicas y asegurar chequeos regulares y otras prácticas preventivas.

F5.- Comunicación electrónica y conectividad: capacidad para asegurar una comunicación eficiente, segura y de fácil acceso entre proveedores y pacientes.

F6.- Apoyo al paciente: capacidad para permitir a los pacientes el acceso a su propio historial médico, proporcionando una educación interactiva a los pacientes, ayudándoles a que realicen sus propias pruebas y controles en el hogar.

F7.- Procesos administrativos: capacidad para usar herramientas administrativas automatizadas, como sistemas de citas médicas.

F8.- Informes y salud de la población: capacidad para responder con mayor rapidez a los requerimientos de informes, incluyendo aquellos que se refieren a la seguridad de los pacientes y al control de enfermedades.

Para graficar todas estas funciones, imaginemos a un paciente menor de edad que en pleno invierno se contagia de un virus que le provoca fiebre y romadizo intenso. Sin embargo, debido a que sus padres están fuera del país, acude a la consulta médica acompañado de su abuela, quien no está al tanto de la alergia a la penicilina de su nieto. En este orden de ideas, la **F1** permitiría prescindir del riesgo de que uno de los dos no advierta oportunamente al doctor, puesto que la información ya estaría disponible de antemano en su computador en un segmento específico referente a las alergias.

Incluso si imaginamos a una abuela acuciosa que desea consultar una segunda opinión en el mismo recinto clínico, de todas formas, gracias a la **F2** el nuevo profesional estaría al tanto de las potenciales reacciones del NNA a la penicilina por el historial del menor en el establecimiento. Si suponemos que este segundo profesional emite una receta, la abuela no tendría razones para afligirse por la calidad ortográfica de esta, ni tendría que padecer las consecuencias de que su nieto la pierda o dañe, debido a que en virtud de la **F3** el formato digital facilitaría la comprensión, como asimismo los riesgos de daño o pérdida. Incluso, en el caso que el profesional no advirtiera que el menor es alérgico, al momento de prescribirle este medicamento, el sistema podría generar una alerta de incompatibilidad de ese fármaco con esta condición específica del menor.

Ahora bien, incluso puestos en la lamentable hipótesis de que el menor contraiga una alergia a la penicilina y como consecuencia de ello genere diversas úlceras cutáneas en el cuerpo, la FCE sería de gran utilidad por cuanto la virtud de la **F4** es que, por ejemplo, todo el equipo médico que intente resolver este caso podría dejar registro digital de los apuntes

que cada profesional genere hasta dar con la solución, además de recordatorios o mensajes internos que sean necesarios.

Además, por medio de la **F5** el equipo médico podría mantener informada a toda la familia, incluyendo a los progenitores que no se encuentran en Chile, a través de una información segura, clara y de fácil acceso que los profesionales podrían mantener disponible en el sitio web del establecimiento o en la plataforma que el Estado provea, según sea el caso.

Por otra parte, si suponemos que este NNA sobrevive a las nocivas consecuencias de la alergia y los doctores le recomiendan reposo domiciliario, él podría ilustrarse personalmente de su caso clínico por medio de las regalías que ofrece la **F6**. Además, si fueren necesarios algunos controles presenciales, tanto él como su abuela tendrían la facultad de agendar sucesivas consultas médicas a través de un sistema en línea y gozar los beneficios de la **F7**. A su vez, el personal médico o administrativo también se vería favorecido, pudiendo monitorear de cerca la evolución del paciente, junto con mantener ordenadas sus respectivas agendas laborales.

Por último, la autoridad sanitaria, en conformidad a la **F8,** tendría la posibilidad de acceder a información en tiempo real respecto de los casos de alergias a medicamentos, los segmentos etarios y socioeconómicos afectados, su distribución en el país, cómo los profesionales los han resuelto, así como también otras estadísticas relacionadas. Estos antecedentes son trascendentales para una correcta y oportuna toma de decisiones en políticas públicas, pudiendo llegar a ser determinantes en la sobrevivencia de algunas personas.

5.- BENEFICIOS DE LA FCEI.

Hasta el momento, ha quedado de manifiesto que las FCE pueden reportar una serie de beneficios para gran parte de la cadena de personas e instituciones que intervienen durante el proceso asistencial. Sin embargo, es posible maximizar aún más sus frutos cuando los sistemas informáticos gozan de interoperabilidad.[65] [66]

En este sentido, los beneficios para el **paciente** consisten en una **(i)** mayor movilidad dentro del sistema sanitario, evitando que sea capturado por una determinada institución de salud

[65] OMS. Global strategy on people-centered and integrated health services, 2016. p. 12.
[66] Fundación IDIS. Estudio de interoperabilidad en el sector sanitario: El paciente como actor principal, 2016. p. 10-11.

que de modo exclusivo posea sus datos. Adicionalmente, la persona podría ser atendida en cualquier región del país, tanto en el sistema público como en el privado, sin el riesgo de que el doctor que realiza la acción de salud no disponga de todos los antecedentes por tratarse de un "paciente nuevo".

Por ello, además, la FCEI es capaz de proveer **(ii)** mayor seguridad para el paciente en su atención de salud, al menos en lo que se relaciona con la correcta provisión de la información, logrando reducir la probabilidad de que se emitan diagnósticos errados.

Relacionado con lo anterior, la FCEI facilita **(iii)** mayor accesibilidad de la información clínica por parte de las personas gracias a una mayor transparencia y certeza en la circulación del historial clínico. Ello, a su vez, genera las condiciones necesarias para que **(iv)** aumente la corresponsabilidad de las personas en su atención de salud y se generen condiciones para que surja la figura del paciente experto.[67] Estos últimos consisten en un "agente activo de salud con un rol educador y facilitador que constituye una fuente importante de apoyo social y emocional para otros pacientes".[68]

En efecto, si suponemos que existen plataformas digitales desde donde los pacientes puedan descargar su información (idealmente proveídas por el Estado) —o que los propios establecimientos médicos tengan la posibilidad de compartirla—, las personas podrían contar con los elementos necesarios para poder velar por su propia salud y complementar el deber que tiene el personal médico en virtud de su juramento hipocrático. En esta línea, el paciente podría exigirle al profesional que lo atiende que le explique en palabras sencillas las razones que justifican su diagnóstico, fiscalizar que el doctor esté interpretando adecuadamente aquello que consta en la ficha clínica, entre otros.

Por ejemplo, un paciente alérgico a un medicamento común como el paracetamol podría verificar con su médico si es que el fármaco que este pretende recetar posee algún compuesto que pudiere generarle una reacción adversa, cuestión que podría marcar la diferencia entre la vida y la muerte.

Otros beneficios para el paciente son el **(v)** aumento en el acceso y puntualidad de la atención por medio de la automatización de los aspectos administrativos de las prestaciones de salud. Adicionalmente, permite **(vi)** disminuir los costos mediante

[67] Op. cit. p. 65.
[68] Op. cit.

diagnósticos precisos que evitan la realización de exámenes médicos innecesarios que, incluso en algunas oportunidades, pueden estar duplicados. Ambas ventajas resultan de gran ayuda en pacientes con patologías crónicas y complejas que requieren atención y exámenes constantemente.

Así las cosas, al lograr compartir la toma de decisiones con los profesionales y potenciar la capacidad de autogestión y control de las condiciones de salud a largo plazo, el paciente disfrutaría en plenitud del sistema de salud, al pasar a estar ubicado en el centro de su diseño".[69] Y, para lograr esto, resulta insalvable potenciar la capacidad de coordinación existente en la red de salud, sobre todo en el tratamiento de las fichas clínicas.

Para ilustrarlo, en un fallo la Corte Suprema estimó que existe falta de servicio por la entrega inoportuna y errada de los resultados de un paciente VIH positivo.[70] En este caso, además, la dilación por cerca de tres años generó que otras personas se contagiaran en el tiempo intermedio, en cuanto el paciente sólo tuvo conocimiento luego de que someterse a un examen particular. El hospital pese que argumentó que la ficha clínica estaba incompleta y desactualizada no pudo evitar ser condenado al pago de veinticinco millones de pesos por daño moral.

Por otro lado, el **personal médico o administrativo**, es beneficiado por la FCEI en cuanto **(i)** el proceso asistencial se torna más eficiente, pudiendo entregar **(ii)** diagnósticos precisos, **(iii)** hacer mejor uso del tiempo y cumplir sus metas de gestión y **(iv)** velar por el adecuado descanso del personal, (v) optimizar sus procesos de registro y notificación a la autoridad sanitaria en aquellos casos en que se encuentren obligados a hacerlo (por ejemplo en las enfermedades de notificación obligatoria).

Lo anterior no es baladí, considerando que la evidencia indica que los turnos prolongados aumentan la probabilidad de que los médicos incurran en conductas erráticas en la emisión de prescripciones médicas[71], lo que se encuentra corroborado por un reciente estudio del *Sheba Medical Center* de Israel, que sostiene que los médicos tienen más del doble de

[69] OMS. Global strategy on people-centered and integrated health services, 2016. p. 12.
[70] SCS Rol Nº 18.253-2017.
[71] LEVIATAN Iliona, OBERMAN Berenice, ZIMLICHMAN Eyal y STEIN Gideon. Associations of physicians' prescribing experience, work hours, and workload with prescription errors, Journal of the American Medical Informatics Association, Volume 28, Issue 6, 2021. pp. 1074-1080.

probabilidades de cometer errores en las prescripciones cuando realizan dos o tres turnos seguidos.[72]

Por consiguiente, en la medida en que el personal médico ejerza su labor teniendo información exacta respecto de los pacientes que atiendan y no tengan lugar jornadas carentes de un descanso suficiente, la FCEI también permitirá la **(vi)** reducción de potenciales conductas generadoras de responsabilidad civil.

Siguiendo esta línea, la FCEI **(vii)** fomenta la existencia de condiciones adecuadas para que la práctica de salud se optimice y, con ello, los resultados sanitarios mejoren. Para ejemplificar de mejor manera: si los profesionales no tuvieren que destinar una parte significativa de la atención médica en intentar reconstruir la historia clínica de los pacientes, el ciclo asistencial sería más exitoso. Por ejemplo, en EE.UU., el cuarto hospital más grande del país (Hackensack UMC) logró un ahorro de 65.000 horas en 2017 al eliminar el uso de papel dentro de los procesos de admisión a urgencias.[73]

Por último, las ventajas de la FCEI pueden ser analizadas desde aquellas que son aprovechadas por el **Estado** en cuanto está mandatado de modo preferente a garantizar la ejecución de las acciones de salud (art. 19 Nº 9 CPR), pero ajustándose a un criterio de coordinación, cuyo fundamento no es solo el texto constitucional, sino que también la maximización de recursos que por definición son escasos, según la Corte Suprema.[74]

En efecto, habida cuenta de que la interoperabilidad permite "intercambiar datos sin errores, interpretar los datos y hacer un uso eficaz de los datos intercambiados", la FCEI le posibilitaría a la Administración del Estado un **(i)** cumplimiento más cabal de las competencias en salud. Por ejemplo, una persona no estaría determinada a atenderse siempre en el mismo lugar porque ahí se almacena su información y, aún en vacaciones, podría acceder a una prestación de salud que guardara relación con su historial clínico.

En este sentido, **(ii)** la eficiencia del proceso asistencial se optimiza propiciando un mayor bienestar para la población sin distinguir por regiones, por cuanto la cobertura se amplía y los resultados de la práctica médica mejoran. Por cierto, esto tiene efectos en la dimensión

[72] A mayor abundamiento, según el estudio, la probabilidad de error en un turno único de ocho horas es de 0,88%, en uno doble de 1,88% y, en un tercero seguido —es decir, 24 horas corridas—, aumenta a 2,1%.
[73] Recurso en línea: DF Salud Nº 32, Mayo 2018, p. 2. Disponible en: https://bit.ly/3ESKyy6. [consulta: 06 febrero 2022]
[74] SCS Rol Nº 34.536-2017, considerando 7º.

fiscal del Estado, ya que la FCEI permite que la Administración pueda **(iii)** tratar los datos de salud según las necesidades que se deriven del conjunto de historias clínicas, sin perjuicio de que esta ventaja pueda transformarse en un peligro, cuestión que será analizada en el Capítulo III.

Ahora bien, gracias al tratamiento de DPS proveídos por la FCE la autoridad podría **(a)** acceder al estado de salud real de la población (estadística), **(b)** potenciar la investigación en salud enfocada en afrontar los principales menesteres de la ciudadanía y **(c)** adoptar mejores decisiones para el diseño e implementación de políticas públicas.

Para ilustrar lo anterior, en virtud de la letra **(a)** el Estado podría detectar y enfrentar oportunamente los efectos nocivos de enfermedades que estén impactando a una parte de la población, como ocurriría con un rotavirus que estadísticamente afecte a una determinada zona de la Región Metropolitana. Mientras tanto, en conformidad a la letra **(b)**, las autoridades competentes podrían fomentar investigaciones para remediar los efectos de este virus.

En cambio, según la letra **(c)**, las autoridades podrían diseñar políticas públicas destinadas a prevenir enfermedades, patologías o trastornos que afecten a una porción significativa de la población (Alzheimer, hipertensión u obesidad, respectivamente) o bien a un segmento específico (dolencias generadas por la influencia ambiental, por ejemplo). A partir de lo anterior, se desprende también un importante **(iv)** ahorro fiscal. En efecto, **(iv)** el Fisco gastará menos mientras más certeros sean los diagnósticos y más sana se encuentre la población, lo que sería posible gracias a la ficha clínica en soporte electrónico e interoperable. Sin embargo, debemos tener presente que resulta ineludible la inversión inicial que sería necesaria para implementar la FCEI en todo el país.

A mayor abundamiento, el CENS sostiene que "la interoperabilidad de los sistemas de salud en Chile podría reportar al país un ahorro de $USD 170 millones, como resultado de una mayor disponibilidad de información a los usuarios y a datos que faciliten una mejor toma de decisiones médicas".[75]

Esta institución se basa en un estudio del consejero de HL7 Internacional y profesor de Harvard, Blackford Middleton quien, junto a otros profesores en 2005, sostuvo que "el

[75] Recurso en línea: Proyectos de Interoperabilidad permitirán ahorro USD170 millones en Chile, 2017. Disponible en: https://bit.ly/3D0RFU1. [consulta: 06 febrero 2022]

ahorro neto que supondría la implantación a nivel nacional de una interoperabilidad totalmente estandarizada entre proveedores y otros cinco tipos de organizaciones podría suponer 77.800 millones de dólares anuales, es decir, aproximadamente el 5 por ciento de los 1,661 billones de dólares que se prevé gastar en la sanidad estadounidense en 2003" (la traducción es nuestra).[76]

Ello corrobora que la interoperabilidad puede ayudar a mejorar radicalmente la gestión del sistema de salud, aspecto que aún es un tema pendiente en EE.UU., donde un tercio del precio total de la atención de salud corresponde a costos burocráticos, llegando a cuadriplicar el precio per cápita que paga, por ejemplo, Canadá en este ítem.[77]

Por otro lado, incluso es posible ahorrar en el bodegaje de incontables fichas clínicas del sistema público de salud y en el pago de todas aquellas demandas contra el Fisco por casos de responsabilidad civil médica referidas al uso inadecuado de las fichas clínicas.

A modo de recapitulación de los beneficios que la FCEI produce para el sistema de salud en su integridad, podemos observar que la OMS identifica los siguientes:

1.- EVITA: el uso innecesario de los centros de salud y tiempos de espera.

2.- MEJORA: equidad en el acceso, la seguridad de los pacientes gracias a la reducción de los errores médicos y malas *praxis*, la precisión en el diagnóstico con el consiguiente efecto en las derivaciones a otros centros de salud.

3.- REDUCE: mortalidad y morbilidad causadas por enfermedades infecciosas y no transmisibles; las hospitalizaciones y el tiempo de los postoperatorios mediante una atención primaria sólida y mejor coordinación de los servicios, el gasto reiterado o duplicado en exámenes, medicamentos u otras prestaciones de salud, así como los costos globales de la atención per cápita.[78]

[76] WALKER, Jan, PAN, Eric, JOHNSTON, Douglas, ADLER-MILSTEIN, Julia, BATES, David y MIDDLETON, Blackford. The Value Of Health Care Information Exchange And Interoperability, Health Affairs (Project Hope), 2005. p. 16.
[77] Recurso en línea disponible en: https://reut.rs/2Yqv04q.
[78] OMS. Global strategy on people-centered and integrated health services, 2016. p. 13.

TABLA RESUMEN DE LOS BENEFICIOS DE LA FCEI PARA LOS DISTINTOS ACTORES						
BENEFICIOS	**CIUDADANO**	**PROFS. SANITARIOS**	**CÍA. SEGUROS**	**PRESTADORES PRIVADOS**	**SERVICIOS SALUD PUBLICA**	**MINSAL**
Accesibilidad a información clínica	✓	✓				
Corresponsabilidad	✓					
Mejora en continuidad asistencial		✓		✓	✓	
Movilidad del paciente en sistema sanitario	✓			✓	✓	
Seguridad del paciente	✓	✓		✓	✓	✓
Mejor práctica clínica		✓				
Mejores resultados salud	✓					
Más eficiencia de procesos asistenciales	✓		✓	✓	✓	✓
Más y mejor investigación		✓				
Cumplimiento de competencias salud					✓	✓

TABLA 4. ELABORACIÓN PROPIA, EN BASE A FUNDACIÓN IDIS (2016).

6.- PRINCIPIOS DE LA INTEROPERABILIDAD.

A. PRINCIPIOS GENERALES DE LA INTEROPERABILIDAD EN TODOS SUS NIVELES (INTRA-ADMINISTRATIVO, VERTICAL, HORIZONTAL Y REGIONAL-TRANSFRONTERIZO).

Las cualidades de la interoperabilidad no surgieron al alero del desarrollo tecnológico de las fichas clínicas, sino que a propósito de iniciativas gubernamentales destinadas a estandarizar las especificaciones técnicas de la totalidad de la Administración del Estado para que la interacción entre esta y la ciudadanía se vea facilitada.

Dicho fenómeno se consolida hacia fines del siglo XX, con el programa de la UE de 1999, que el año 2004 sería reemplazado por la primera regulación marco sobre interoperabilidad,

denominada “prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y ciudadanos (IDABC)”.[79] [80]

Paralelamente, en julio de 2002, la *Federal Chief Information Officers Council* de EE.UU. impulsa el *Egovernment Enterprise Architecture Guidance* para orientar proyectos marco sobre interoperabilidad a nivel nacional.[81]

En la actualidad, el principal modelo global de interoperabilidad corresponde al Marco Europeo de Interoperabilidad que se inclina hacia la obtención de la plena digitalización de los servicios públicos comunitarios. Ello, en el entendido de que la libre circulación de mercancías, servicios, capital y personas por la que aboga la regulación comunitaria, requiere de servicios públicos digitales eficaces, eficientes y de alta calidad que no generen burocracia y gastos excesivos.[82]

Para satisfacer este propósito, el EIF concretamente “proporciona orientación, mediante un conjunto de recomendaciones, a las administraciones públicas sobre cómo mejorar la gobernanza de sus actividades de interoperabilidad, establecer relaciones entre organizaciones, racionalizar los procesos que dan soporte a los servicios digitales de extremo a extremo y garantizar que la legislación nueva y la legislación en vigor no comprometan los esfuerzos de interoperabilidad”.[83] Estas recomendaciones se sostienen sobre la base de determinados principios cuyo cumplimiento es imprescindible para el establecimiento de servicios públicos interoperables. [84]

No obstante, debido a que algunos de los principios responden exclusivamente a las complejidades particulares de la de UE, nos hemos centrado en los principios que, de acuerdo con el contexto nacional y regional de Chile, consideramos más pertinentes; estos se encuentran subdivididos en tres grupos: los que configuran el contenido nuclear de la

[79] Decisión 1720/1999/CE del Parlamento Europeo y del Consejo de 12 de julio de 1999 por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), así como el acceso a las mismas.
[80] Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC).
[81] GUIJARRO, Luis. 2007. Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States, Government Information Quarterly, Volume 24, Issue 1, p. 10.
[82] EIF, 2017. p. 4.
[83] Op. Cit.
[84] Op. Cit.

interoperabilidad; aquellos que reflejan las necesidades y expectativas genéricas de los usuarios; y, finalmente, aquellos que componen las bases para la cooperación entre las administraciones públicas.

i. Principios que configuran el contenido nuclear de la interoperabilidad.

El primer subgrupo comienza con el (i) **principio de apertura**, cuyo concepto está redirigido hacia tres tipos o clases. En primer lugar, apunta hacia la apertura de los datos que tratan las diversas administraciones —denominados "datos abiertos"—. En este sentido, la regla general es que los datos sean abiertos, de modo que las personas los puedan usar y reutilizar a no ser exista alguna restricción que obligue a lo contrario, como serían los datos personales sensibles o normas que impongan el respeto a un deber de confidencialidad.

En segundo lugar, hace referencia a la apertura en el uso de *softwares*, debido a que provenir de fuentes abiertas permite reducir costos que deben soportar las arcas públicas. Además, evita o disminuye la probabilidad de que la Administración sea capturada por un determinado proveedor, con todos los riesgos que se derivan.

En tercer y último lugar, el principio apunta hacia la apertura de especificaciones o normas en cuanto posibilita un mayor escrutinio y aporte de parte de la ciudadanía. En este orden de ideas, se trata de que los ciudadanos y empresas participen en el diseño de nuevos servicios y cooperen en la perfección de los que ya estén funcionando.

El (ii) **principio de transparencia** tiene por objeto que los organismos que conforman la Administración del Estado adquieran visibilidad, de modo que las personas puedan ver y entender las normas, procesos, datos, toma de decisiones y servicios. Además, busca garantizar la disponibilidad de interfaces con los sistemas de información internos y asegurar el derecho a la PDP.

En tanto, el (iii) **principio de reutilización** releva la importancia del *know how* que se va generando al alero de cada servicio público digital, así como la información que cada uno va recopilando o desarrollando. En efecto, se trata de que, cuando los organismos enfrenten un problema, exista la posibilidad de que se apoyen en el trabajo previo de otras entidades públicas, aplicando soluciones que hayan demostrado ser satisfactorias en casos semejantes. Lo propio ocurre con la información, de modo que los organismos —en caso de ser necesario— puedan acceder y tratar datos que otra institución genera. Para estos

efectos, resulta imprescindible que las entidades que conforman las administraciones generen canales adecuados para compartir sus soluciones técnicas y cooperen entre sí para el desarrollo de soluciones conjuntas para la implantación de los servicios públicos europeos.

El núcleo de la interoperabilidad finaliza con el (iv) **principio de neutralidad tecnológica y portabilidad de los datos**, que busca asegurar que las entidades públicas eviten inclinarse por una solución técnica específica y que se mantenga latente la posibilidad de que estas se adapten a nuevas innovaciones que ofrece el desarrollo tecnológico. Esto se manifiesta en que las administraciones deben permitir el acceso a sus servicios y datos con independencia de cualquier tecnología o producto concreto y también posibilitar su reutilización. En consecuencia, no se verificaría este principio en el supuesto de que un servicio público exija un determinado sistema operativo para poder realizar averiguaciones.

La portabilidad, por su parte, se encarga de garantizar la libre circulación de los datos personales de los usuarios de los servicios públicos europeos, evitando que su transferencia entre sistemas y aplicaciones sea engorrosa, lo que se cimenta en la convicción de que los datos son inherentes a los titulares, quienes son libres para gestionarlos a su antojo en la medida en que se respeten las normas sobre PDP (GDPR).

ii. PRINCIPIOS REFLEJAN LAS NECESIDADES Y EXPECTATIVAS GENÉRICAS DE LOS USUARIOS.

El primer principio de este subgrupo corresponde a la (i) **primacía del usuario**, cuyas prerrogativas están dirigidas a que sean las necesidades y exigencias de los propios usuarios las que orienten el diseño y desarrollo de los servicios públicos europeos. Además, requiere, por ejemplo, que se contemplen varios medios para prestar el servicio, pudiendo los usuarios elegir el que mejor se adecúe a sus necesidades, o bien que la información sea solicitada por una sola vez a las personas.

En relación con lo anterior, se contempla el principio de (ii) **inclusión y accesibilidad** que pretende —en el caso de la inclusión— que todos los usuarios de los servicios públicos europeos puedan acceder y gozar de estos en igualdad de condiciones; mientras que el principio de accesibilidad se concentra en garantizar que las oportunidades para acceder a los servicios públicos sean las mismas para todos los ciudadanos. Esto necesariamente demanda crear condiciones para que grupos especialmente discriminados o

tradicionalmente excluidos, como personas de tercera edad, discapacitados, extranjeros —incluso cuando estos factores confluyen en forma interseccional—, puedan acceder a los servicios públicos europeos.

Por otra parte, el principio de (iii) **seguridad e intimidad**, exige garantizar estos derechos respecto de las personas que acceden a los servicios públicos europeos. En consecuencia, el EIF aboga por el establecimiento de marcos comunes de seguridad e intimidad —tales como el GDPR— para garantizar el intercambio de datos seguro y fiable entre las administraciones públicas y en interacciones con los ciudadanos y las empresas.

Finalmente, en el contexto europeo resulta importante el principio de **(iv) multilingüismo**, que mandata a las administraciones públicas a que estén dotadas de sistemas de información capaces de operar con una cantidad de idiomas acorde a los usuarios previstos.

iii. Principios que aportan una base para la cooperación entre las distintas administraciones públicas europeas (10 a 12).

Para propiciar la cooperación entre las distintas administraciones europeas, se contempla el principio de (i) **simplificación administrativa**, cuyos ejes son dos: "servicios digitales por defecto" (*Digital-by-default*), destinado a garantizar que siempre exista un canal digital disponible para acceder a un servicio público europeo y "digital primero" (*digital first),* orientado a la convivencia de los canales físicos con los digitales, sin perjuicio de que estos últimos tengan prioridad.

La simplificación administrativa tiene por objeto racionalizar y facilitar los procedimientos administrativos para reducir la carga que estos ejercen sobre las administraciones públicas, las empresas y los ciudadanos.

El principio de **(ii) conservación de la información** busca asegurar que los documentos y otros antecedentes conserven su legibilidad, fiabilidad e integridad, de manera que las personas puedan acceder a ellos durante todo el tiempo que lo exijan las normas relativas al principio de seguridad e intimidad. Esto resulta especialmente delicado, considerando que la información es intercambiada en diversos países.

El último principio de este subgrupo corresponde al de (iii) **evaluación de efectividad y eficiencia**, referente a las soluciones de interoperabilidad y opciones tecnológicas

disponibles para los servicios públicos europeos, debiendo tener presente las necesidades de los usuarios, la proporcionalidad y equilibrio entre costos y beneficios. Este dinámico principio inspira todo el proceso de implementación de la interoperabilidad en la UE.

Al respecto, cabe tener presente que en el borrador impulsado el año 2017 por la SEGPRES —denominado "Norma Técnica de Interoperabilidad en el Estado de Chile" y que, finalmente, nunca llegaría a ser publicado— sí se consideraban principios como los de colaboración, estandarización, equivalencia funcional, gratuidad, finalidad, competencia, seguridad de la información y tratamiento de la información.[85] A todas luces, la entrada en vigencia de una normativa como la precitada hubiese resultado un aporte significativo, en miras a una eventual regulación de la interoperabilidad en el Estado, así como en el área de la salud.

Sin embargo, es de esperar que a través del reglamento de transformación digital estos defectos se enmienden en cuanto obliga a que los órganos de la Administración del Estado habiliten servicios de interoperabilidad, junto con exigir que, en el proceso de elaboración de normas técnicas, la SEGPRES deba necesariamente considerar los estándares internacionales existentes.

B. Principios de la interoperabilidad en el área de salud y las fichas clínicas.

Ahora bien, corresponde hacernos cargo de los principios de la interoperabilidad que específicamente corresponden al área de salud, incluyendo a las fichas clínicas. En este sentido, la OMS, el año 2016 impulsó la "*Global strategy on people centered and integrated health services",* cuyo paradigma es el establecimiento de un sistema de salud integrado y centrado en la persona; para esto, encarga el respeto a determinados principios.[86]

Entre los centrales está velar por un sistema de salud que ofrezca una atención (i) **integral**, que no solo responda a las necesidades de las personas, sino que también logre adaptarse según como estas vayan evolucionando en el tiempo. Para tales efectos, resulta primordial garantizar el acceso (ii) **equitativo**, (iii) **continuo**, (iv) **coordinado** y (v) **sostenible**. Ello implica que todos los actores que componen el sistema de salud deban estar sincronizados

[85] Recurso en línea disponible en: https://bit.ly/3D4OfzS. [consulta: 06 febrero 2022]
[86] OMS. Global strategy on people-centered and integrated health services, 2016. p. 11.

en torno a criterios de eficiencia y eficacia, de modo que la atención esté disponible para todos y en todo momento, pudiendo mantenerse dichas condiciones en el tiempo.

La coordinación entre los diversos actores es relevante para poder materializar un sistema de salud enfocado en la (vi) **prevención**, especialmente respecto de aquellas personas cuyos determinantes socioeconómicos las ubican en una posición de mayor indefensión.

Por otra parte, resulta fundamental abogar por un sistema de salud (vii) holístico que pueda afrontar las afectaciones en el bienestar de las personas en sus distintas dimensiones, ya sea físico, mental o emocional. Lo anterior demanda equipos médicos (viii) colaborativos entre la atención primaria, secundaria y terciaria, así como con otros sectores, recordando que el personal administrativo también juega un rol trascendental para estos efectos.

La OMS también subraya el diseño de sistemas orientados hacia el (ix) **cumplimiento de los objetivos**, que no es otro que el (x) **empoderamiento de las personas en la gestión y responsabilidad de su propia salud**. Esto requiere cuantificar y evaluar los resultados a lo largo del tiempo y la generación constante de nuevos incentivos destinados a impulsar la capacidad autogestión de cada persona en relación con su salud.

Por último, debe garantizarse el (xi) **respeto del sistema de salud hacia la dignidad de las personas**, sin que las diferencias socioeconómicas, culturales u otras puedan atentar contra este fin principal.

7.- BARRERAS.[87]

La interoperabilidad constituye una solución técnica que es capaz de beneficiar a todos los actores del sistema de salud, sin embargo, en su proceso de implementación surgen diversas barreras que obstaculizan su avance y que es necesario considerar.

Para la compañía MINSAIT (2021) existen seis principales barreras. La primera corresponde a la **selección de estándares**, por cuanto existe una multiplicidad de alternativas, pero no todas están internacionalmente aceptadas. Esto puede resultar problemático, debido a que no todas las regiones o países tienen los mismos estándares en materia de PDP y ciberseguridad.

[87] MINSAIT. Libro blanco de interoperabilidad en salud. América Latina. Edición 2020-2021, 2021. p. 15.

En segundo lugar, mencionan la **coexistencia de sistemas informáticos**, puesto que la convivencia de distintos sistemas de gestión de la información entre los diversos centros clínicos u hospitalarios que configuran la red de salud merma las posibilidades de homogeneizar y consolidar la información: mientras más disgregada se encuentre la información, mayores dificultades tendrá el personal —tanto médico como administrativo— para llevar realizar su trabajo. Asimismo, esta dispersión también aumenta las chances de que se generen hipótesis de responsabilidad civil.

Asimismo, entre los distintos sistemas informáticos, así como dentro de estos, resulta imprescindible homogeneizar o tender hacia una misma nomenclatura, de lo contario la información clínica pierde utilidad e incluso puede llevar a que el personal cometa errores, con el consecuente daño a los pacientes.

En tercer lugar, los costos económicos que demanda una adecuada implementación de la interoperabilidad es un factor que puede motivar a la autoridad para inhibirse en su toma de decisiones, privilegiando otro tipo de gastos. A ello se suma que los beneficios de esta inversión no son instantáneos, sino que sus resultados se podrán visualizar a mediano o largo plazo, lo que se extiende a los réditos políticos que una autoridad legítimamente podría esperar obtener.

Por otra parte, sabemos que el establecimiento de la interoperabilidad para las fichas conlleva incontables beneficios, aunque debemos considerar que ello puede colisionar con determinados intereses. Así, la cuarta barrera de la interoperabilidad la constituyen los **intereses contrarios a los beneficios que de esta se desprenden**; esto se manifiesta en que la interoperabilidad implica una mayor circulación de los datos personales de los usuarios del sistema de salud, con ello se dificulta la cautividad de la información que algunas entidades —públicas o privadas— podrían tener o pretender. De ahí que cualquier iniciativa que busque potenciar la titularidad de los datos personales por parte de cada persona tendrá por efecto atentar contra aquellos intereses.

Esto resulta notorio en el caso de ciertas empresas que en la actualidad ofrecen servicios de digitalización e interoperabilidad para determinados centros o redes de salud debido a que, a raíz de la prestación de este servicio, tienen la posibilidad de acceder a valiosa información personal sin que existan garantías palpables de que esa información sensible no será tratada posteriormente con fines comerciales y, por cierto, ilícitos. Esto significa no solo que las personas pierdan autonomía respecto de sus datos personales, sino que

también queden en una posición de indefensión, considerando que terceras personas potencialmente podrían tomar ventaja de dicha información. Por ejemplo, alguien podría subir los precios de aquellos medicamentos respecto de los cuales están en conocimiento que personas identificadas dependen (*targeting*). En relación con esto, podría ocurrir que entre el personal médico o administrativo la implementación de la FCEI produzca cierta incomodidad por los mayores niveles de transparencia, así como escrutinio o *accountability* sobre las labores a las que estarán sometidos.

Los intereses contrapuestos también se pueden explicar con ocasión del bodegaje. De hecho, en la actualidad para almacenar y mantener fácilmente accesibles las fichas clínicas en soporte papel es un requisito *sine qua non* contar con bodegaje y los costos que ello apareja, que en algunos casos pueden ser significativos. Este obstáculo desaparece una vez que se implementa la interoperabilidad, porque el bodegaje se limita a los costos periódicos que implican las nubes digitales.

En síntesis, la implementación de la interoperabilidad se traduce en una pérdida de autonomía para algunos y en la recuperación de esta respecto de otros. En el caso de entidades públicas o privadas que tengan interés en disponer de los datos personales de los pacientes o generar negocios con las fichas clínicas en papel, ven disminuido su albedrío. En cambio, los pacientes recuperan su autonomía en cuanto son titulares de sus propios datos personales, pudiendo disfrutar con mayor libertad las prestaciones ofrecidas por todo el sistema de salud, sin correr el riesgo de que sus datos sean cedidos a terceros que pueden realizar actos perjudiciales con ellos. Así, queda claramente de manifiesto que quienes se opondrán a la implementación de la interoperabilidad serán quienes pierden autonomía y no quienes la recuperan.

Ahora bien, la quinta barrera que identifica la compañía MINSAIT es la **PDP y ciberseguridad**, debido a que la interoperabilidad obliga no solo a invertir en su implementación, sino que también en cumplimiento normativo o *compliance* para adoptar mayores y mejores estándares sobre la materia. Este mayor desembolso puede significar un desincentivo para el desarrollo de fichas clínicas integradas.

Finalmente, la última barrera corresponde a la **preparación del personal** que resulta imprescindible para que los sistemas interoperables de fichas clínicas funcionen y se mantengan adecuadamente en el tiempo.

A las ya mencionadas, sumamos las barreras legales, teniendo en cuenta las circunstancias en las que se desarrolla nuestro país, donde no existe una ley marco de interoperabilidad ni una ley de datos personales moderna o de ciberseguridad, y en ambos casos sin la correspondiente institucionalidad.

Para finalizar, adjuntamos esta tabla elaborada por la CEPAL que resulta esclarecedora, puesto que sintetiza las principales barreras para la interoperabilidad.[88]

BARRERAS PARA LA INTEROPERABILIDAD	
Barreras de competencia	El personal médico o administrativo carece de competencias, dedicación y atribuciones suficientes para impulsar la interoperabilidad, siendo imprescindible invertir en su capacitación para operar y mantener correctamente los sistemas.
Barreras tecnológicas	Está conformada por la multiplicidad de estándares y la coexistencia de distintos sistemas de gestión de información de salud entre las instituciones públicas o privadas.
Barreras conceptuales	Las entidades encargadas de construir las fichas clínicas poseen distintas conceptualizaciones e interpretaciones de la información que incorporan, dificultando una significación unívoca propia de la ciencia.
Barreras organizacionales	A nivel interno, los recintos asistenciales públicos o privados no poseen la misma estructura y jerarquías dificultando el componente administrativo necesario para integrar la información.
Barreras legales	La interoperabilidad debe ser implementada sobre la base de un determinado marco jurídico que la sustente y la inexistencia de uno —como el caso chileno— se erige como un impedimento mayor.
Barreras por pérdida de autonomía	La implementación de la interoperabilidad colisiona con los intereses de determinados actores del sistema de salud que ven disminuida su autonomía como consecuencia de una mayor circulación de los DPS.
Barreras culturales	Compartir información implica un mayor escrutinio acerca de las labores que cada uno de los eslabones del sistema de salud ejerce, lo que puede generar cierta reticencia de parte de ellos para desarrollar iniciativas que se traduzcan en una mayor disponibilidad de la información de salud. Asimismo, no es posible evitar que la implementación de la interoperabilidad deba lidiar con las brechas digitales existentes en el país, particularmente en zonas extremas o lugares con condiciones naturales hostiles. En consecuencia, el proceso de abandono del soporte papel y reemplazo por uno de carácter electrónico no es automático, sino que puede demorar un plazo indeterminado.

TABLA 5. ELABORACIÓN PROPIA, EN BASE A CEPAL (2021) Y FUNDACIÓN IDIS (2016)

A ello se suman los costos de la transición entre las fichas papel y las digitales, que incluye costos financieros y de adaptación de los cuerpos profesionales.

8.- ESTÁNDARES.

[88] CEPAL. Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación, 2021. p. 28-29.

Frente a la multiplicidad de estándares existentes, optamos por basarnos en el predominante a nivel mundial: el *Health Level* 7.[89] Para facilitar la comprensión, analizaremos cada nivel de la interoperabilidad a la luz de las exigencias que respectivamente demanda el precitado estándar:

a. **Estándar para la interoperabilidad técnica:** como se ha señalado, esta clase de interoperabilidad transmite la información de máquina a máquina, sin considerar el contenido del mensaje.[90] De este modo, lo principal para este nivel pasa a ser el *software* utilizado, respecto de los cuales existen diversas alternativas como podrían ser XML/JSON/SOA/TCP/IP/WebServices.

b. **Estándar para la interoperabilidad sintáctica[91]:** considerando que debe existir una sintaxis en la información intercambiada, es necesario distinguir entre mensajes y documentos.
   i. **Mensajería:** el HL7 V2 o V3 estructura homogéneamente la información de los pacientes que consta en las fichas y que posteriormente circulan en los sistemas. Actualmente, el uso del estándar HI7 v2 es bajo; se utiliza, por ejemplo, en Radiología para comunicar el PACS centralizado de MINSAL con los HIS de los hospitales o directamente con los PACS.[92]
   ii. **Documentos**: (i) **CDA** los documentos almacenados son inscritos por personas que pueden no estar habituadas a la plataforma que un ingeniero registra y, en consecuencia, la siguiente persona que acceda al documento no podrá dar fe de la veracidad de los ingresos o datos. Con este estándar es posible saber quién los creó, para quién, cuándo, dónde y sobre qué tema. En caso de que exista alguna duda, se puede trazar con quien introdujo los cambios.[93] (ii) Otro equivalente es el

[89] La definición de HL7 según la NT Nº 820 señala que son "normas relacionadas para la integración, intercambio y recuperación de la información de salud electrónica. Estas normas definen cómo se empaqueta y se comunica de una parte a otra, el establecimiento de los tipos de lenguaje, estructura y datos necesarios para la perfecta integración entre los sistemas de información. […] apoyan la práctica clínica y la gestión, prestación y evaluación de los servicios de salud, y son reconocidos como los más utilizados en el mundo".
[90] PAHO. Revisión de estándares de interoperabilidad para la eSalud en Latinoamérica y el Caribe, PAHO y Oficina Regional para las Américas de la OMS, Washington, D.C., EE.UU., 2016. p. 17.
[91] Recurso en línea: Interoperabilidad Sintáctica CTD CORFO. Disponible en: https://bit.ly/3BR7USg. [consulta: 06 febrero 2022]
[92] RACSEL. Manual estándares interoperabilidad en salud: Recomendaciones técnicas, 2019. p. 75.
[93] BENSON, Tim y GRIEVE, Grahame. Principles of health interoperability: SNOMED CT, HL7 and FHIR, 2021. p. 233.

CCD, que permite comunicar resúmenes clínicos con información estandarizada.[94] Actualmente, en Chile el uso del estándar CDA es muy bajo —siendo utilizado, principalmente, para informes de alta, documentos clínicos y diagnósticos—, debido a que todavía un número importante de instituciones sanitarias trabaja con papel.[95]

iii. **Imágenes**: **DICOM.** Define los formatos de imágenes intercambiables con sus datos y cualidad necesaria para el uso médico.[96] Se puede usar para las resonancias magnéticas, radiografías, medicina nuclear, ultrasonido, así como también para cualquier otro examen cuyo resultado se plasme en una imagen. En Chile, el uso del estándar DICOM es alto, principalmente para radiografía, tomografía o medicina nuclear.[97]

c. **Estándar para la interoperabilidad semántica:**[98] recordando que en este nivel la interoperabilidad vela por el significado, precisión y calidad de la información intercambiada, desde la comunidad internacional han surgido diversos estándares para homogeneizar los términos. El principal corresponde al **SNOMED-CT**, en el que los conceptos pasan a ser lo primordial. Cada uno se define por un identificador de nueve dígitos (SNOMED CT IDENTIFIER o SCTID por sus siglas).[99] Cada concepto SNOMED CT tiene un único y legible *Fully Specified Name* que desglosa a las siglas de nueve dígitos, en caso de necesitar profundizar en alguno de ellos. Otros estándares relevantes que podemos mencionar son: **LOINC**, **IHE** e **ICD-11**.

d. **Estándar de interoperabilidad organizativa:** destacamos la **ISO 13940**, la *HL7 Clinical Context Management* (**CCOW**), ***HL7 EHR System Functional Model*** y **IHE**.

Actualmente, uno de los estándares más utilizados corresponde al HL7 FHIR. Corresponde a un estándar de interoperabilidad moderno, que combina lo mejor de HL7 V2, HL7 V3 y CDA y se enfoca en facilitar su implementación. Usa los estándares web más frecuentes,

[94]Op. Cit. p. 250.
[95] RACSEL. Manual estándares interoperabilidad en salud: Recomendaciones técnicas, 2019. p. 79.
[96] BENSON, Tim y GRIEVE, Grahame. Principles of health interoperability: SNOMED CT, HL7 and FHIR, 2021. p. 437.
[97] RACSEL. Manual estándares interoperabilidad en salud: Recomendaciones técnicas, 2019. p. 81.
[98] Recurso en línea: Interoperabilidad Semántica CTD CORFO. Disponible en: https://bit.ly/3CZ1zpk. [consulta: 06 febrero 2022]
[99] BRAUNSTEIN, Mark. Health Informatics on FHIR: How HL7's New API is Transforming Healthcare, 2018. p. 146.

como XML, JSON y HTTP. Se estructura sobre la base de *resources* o bloques de construcción de todos los intercambios de información en FHIR; cada uno de ellos representa un concepto dentro de la realidad de la atención sanitaria, por ejemplo, pacientes, citas, resultados de exámenes médicos, etc.[100]

Los estándares de interoperabilidad existen y están disponibles para ser utilizados en Chile.

ESTÁNDARES PRIMARIOS DEL HL7		
	CONCEPTO	**CARACTERISTICAS**
HL7 Versión 2	Este estándar de mensajería es el más usado en el mundo. Es soportado por la mayoría de los sistemas presentes en atención sanitaria. Sus ventajas son que es compatible con la mayoría de las interfaces comunes utilizadas en la industria de la salud a nivel mundial.	- Proporciona un marco para las negociaciones. - Reduce costos de implementación. - Su primera versión es de 1987 y la más reciente corresponde a la v2.8.2. - Los mensajes más utilizados en esta versión son los ADT (para admisión de pacientes), los ORGM o OMG (para solicitudes de órdenes) y los ORU (para enviar informes de resultados de laboratorio o de imagen).
HL7 Versión 3	El HL7 v. 3 abarca las terminologías, tipos de datos y la mensajería necesarios para una implementación completa. Está basado en el modelo de referencia HL7 RIM.	- Se centra en la interoperabilidad semántica al asegurar que los sistemas de envío y recepción compartan el mismo significado. - Diseñado para ser una aplicación universal que permite intercambiar mensajes y documentos expresados en sintaxis XML y con una misma terminología. - Su primera versión es de 2005 y la más reciente de 2017. - El Servicio Nacional de Salud del Reino Unido, de Holanda y Canadá lo ocupan actualmente.
CDA Release 2	Estándar de marcado de documentos que especifica la estructura y la semántica de documentos clínicos a los efectos del intercambio entre los profesionales sanitarios y los pacientes. Un CDA puede contener documentos clínicos de todo tipo, tanto con contenido sin estructurar como estructurado y totalmente codificado. La especificación de intercambio de documentos se basa en la utilización de XML, el modelo de información de HL7 (RIM), la metodología de HL7 V3 y el uso de vocabularios controlados o locales como SNOMED CT, ICD, LOINC, etc.	- La versión 2.0 fue publicada en 2005 y es la más reciente. - Persistencia: un documento clínico continúa existiendo sin alteraciones por un periodo de tiempo definido pro-requerimientos locales y regulatorios. - Responsabilidad: un documento clínico debe ser mantenido por una organización a la que se le asigna su cuidado. - Potencial para su autenticación: un documento clínico es un paquete de información que tiene prevista su autenticación legal. - Contexto: un documento clínico establece un contexto para su contenido, ya sea para los pacientes, prestadores u otros. - Completitud: la autenticación o firma de un documento clínico aplica a todo su contenido y no a porciones de este sin el contexto del documento. - Legibilidad: el documento debe poder ser leído por seres humanos sin problemas.
HL7 FHIR	FHIR trata lo mejor de cada estándar vigente en HL7 International (focalizándose en v.2, v.3 y CDA R2) y se basa en estándares web modernos como REST y en recursos (*resources*) o componentes modulares que se combinan en sistemas para resolver problemas reales de atención sanitaria.	- La primera versión es de 2011 y la última de 2019. - Los recursos tienen una forma común de definir y representar debido a que se construyen a partir de tipos de datos que delimitan patrones comunes y reutilizables. - Los recursos tienen un conjunto común de metadatos. - Los recursos tienen una parte legible por humanos. - El FHIR se basa en un enfoque de composición según quien lo implemente (HL7 V.3 es de restricción). - Los recursos pueden ser de administración, medicamentos, financieros, terminología, seguridad y privacidad, entre otros.

[100] Recurso en línea disponible en: https://bit.ly/3mYDWHX. [consulta: 06 febrero 2022]

CCOW	CCOW o *Clinical Context Object Workgroup* es un estándar que pretende facilitar la integración de aplicaciones a nivel de uso mediante una técnica llamada *Context Management*. Permite sincronizar a nivel de interfaz de usuario la información de diferentes sistemas referida al mismo paciente, procedimiento o usuario.	- La primera versión (V.1.0) es de 1998 y fue creada por la Universidad de Duke. La última es la V.1.6, en vigencia desde el año 2017. - Es ideal para instalaciones con más de un sistema informático para información clínica. - Ofrece acceso intuitivo a toda la información. - Aumenta la seguridad del paciente. - Elimina entradas repetidas y duplicadas. - Aplicación fácil de usar.

TABLA 6. FUENTE: RACSEL (2019), CADUCEUS (2018) Y WWW.HL7.ORG.

El CENS ha promovido el conocimiento del estándar HL7 FHIR, por medio de una plataforma digital denominada Huemul, desarrollada en conjunto con la fundación HL7.[101] A través de Huemul se busca facilitar el perfeccionamiento de capital humano por medio de talleres interactivos de autoevaluación y permite la validación oficial de los conocimientos en HL7 FHIR.[102] Todo lo anterior se sostiene sobre la base de la necesidad de masificar el uso de historias clínicas interoperables, para lo cual el capital humano resulta trascendental y, como hemos visto, es tan solo una de las aristas.

9.- CONJUNTO MÍNIMO O BÁSICO DE DATOS (CMBD).

Una manera de armonizar los estándares abordados precedentemente es a través del conjunto mínimo o básico de datos, que surge en 1981 en la Comisión de las Comunidades Europeas con apoyo de la OMS y otras organizaciones como la Asociación Europea de Informática Médica. En esa oportunidad se definió como un "núcleo de información mínima y común sobre los episodios de hospitalización".[103] Estos, a nivel comparado, están contemplados en el marco del denominado Resumen del Paciente o la Historia Clínica Resumida, los que resultan trascendentales para comunicar dicha información, tanto a nivel nacional como internacional. En términos sencillos, consisten en "un conjunto de datos médicos básico de un paciente que incluye los hechos clínicos más importantes necesarios para garantizar una asistencia sanitaria segura".[104]

[101] De acuerdo con el CENS, el año 2018 su área de interoperabilidad impulsó una serie de tutoriales gratuitos para desarrolladores en cuatro regiones del país destinados a comprender la aplicación del estándar HL7. Sin embargo, cada ejercicio de los talleres demandaba más de dos horas en ser corregido. De ahí nace esta iniciativa digital. Recurso en línea disponible en: https://bit.ly/3EVtEhD. [consulta: 06 febrero 2022]

[102] Recurso en línea: Huemul – Primera plataforma chilena para aprender HL7 FHIR. Disponible en: https://bit.ly/3bQFXj5. [consulta: 06 febrero 2022]

[103] Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada. A diferencia de Chile, el artículo 5º considera treinta y un datos obligatorios para este registro.

[104] RACSEL. Manual estándares interoperabilidad en salud: Recomendaciones técnicas, 2019. p. 16.

Para graficar su importancia, recurrimos al siguiente ejemplo: puede ocurrir que un paciente alérgico a un medicamento común, como el paracetamol o la penicilina, durante un viaje requiera ser atendido y resultará esencial que el profesional disponga de esta información, capaz de determinar la sobrevivencia de la persona.

En Chile, el CMBD ha sido definido por la NT 820 de 2016 emitida por el MINSAL, sobre Estándares de Información de Salud, como "el conjunto de variables necesarias para el registro de los datos administrativos y clínicos, que se capturan en diferentes etapas del proceso de atención en la Red de Servicios de Salud".[105] Esto se enmarca en la Agenda Digital 2020, que incluyó la "definición del conjunto mínimo básico de datos de la ficha clínica electrónica, que constituya la base de la interoperabilidad de la red asistencial", dentro del capítulo 26 referente al "Sistema de Informatización de la Red Asistencial: Ficha médica electrónica".[106] Este propósito fue materializado en julio de 2017.[107]

En un contexto en el que la cantidad de información abunda, la ventaja de la uniformidad de sus términos consiste en velar porque la precisión y la calidad de ella sean ideales para el funcionamiento clínico y administrativo. Así, es posible gestionar el problema del exceso de información que afecta a todo el personal médico o administrativo, favoreciendo a todos los niveles de interoperabilidad, en especial a la semántica, aspecto en que lo importante es el contenido del mensaje que un emisor envía a un receptor.

En la NT se reconoce que "la adopción de la estandarización permite diseñar, implementar y mantener actualizados, sistemas de información, capaces de proporcionar datos estadísticos para la formulación, control y evaluación de diferentes programas y los impactos directos que sus acciones generen sobre el estado de salud de la población y la calidad de la atención". El CENS considera que el objetivo del CMBD es "la normalización del conjunto mínimo de datos necesarios para asegurar la trazabilidad financiera y sanitaria de aquellos beneficiarios que son atendidos en la red de prestadores públicos y privados del país".[108] De esta forma, se definen una serie de datos y vocabularios basales que pueden ser utilizados por uno o más CMBD. En el caso de las personas que solicitan

[105] Decreto Exento Nº 643 que sustituye norma técnica sobre estándares de información de salud de fecha 30 de diciembre de 2016.
[106] Recurso en línea disponible en: https://bit.ly/3wu9eth. [consulta: 06 febrero 2022]
[107] Recurso en línea disponible en: https://bit.ly/3o7yjXi. [consulta: 06 febrero 2022]
[108] Recurso en línea: Guía implementación CMDB, CENS, 2017. p.8. Disponible en: https://bit.ly/3EWLHUJ. [consulta: 06 febrero 2022]

atención, los datos obligatorios (previamente definidos con sus códigos y glosas respectivas) son los siguientes:

CMBD — ESTÁNDARES DE DATOS DE LA PERSONA			
Datos de identificación	Nombres	**Datos de ubicación**	Código de Región
	Primer apellido		Código de Provincia
	Segundo apellido		Código de Comuna
	Run		Código de Límite Urbano Censal
	Dígito verificador		Código de Religiones o Cultos
	Edad año		Código Vía de la Dirección
	Edad mes		Nombre de la Vía
	Edad día		Número de Dirección
	Edad hora		Código Complemento Dirección
	Edad minuto		Complemento Dirección
	Pasaporte		Latitud
	Otra identificación		Longitud
	Fecha de nacimiento		Código Postal
	Código de sexo		
	Código de país de origen		
	Código de nacionalidad		
Datos relativos a características personales	Código de Estado Civil	**Datos de contacto**	Teléfono Fijo
	Código de Pueblo Indígena Declarado		Teléfono Móvil
	Código de Religión o Culto Declarado		Correo Electrónico
Datos académicos y profesionales	Código de Nivel de Instrucción	**Datos de Sistema de Salud**	Código de Previsión de Salud
Datos de trabajo	Código de Categoría Ocupacional		Código de Modalidad de atención Fonasa
	Código de Ocupación		Código de Tramo Fonasa
	Código de Nivel de instrucción		Código Leyes Previsionales

TABLA 7. ELABORACIÓN PROPIA, EN BASE A DECRETO EXENTO Nº 643, P. 46-47.

Existen CMBD para prestadores individuales, es decir, personas naturales que poseen una profesión legalmente habilitada para ejercer su rol en materia de salud, según el Decreto Exento Nº 643.

Resulta necesario advertir que la estandarización de los conceptos es solo un paso para lograr la interoperabilidad en todos los niveles, de modo que las políticas públicas impulsadas por el Estado en salud estén integradas. En este sentido, el esfuerzo que se haga para el desarrollo de los CMBD no debe dejar de avanzar la implementación de estándares internacionales para el nivel técnico, sintáctico, semántico u organizativo, porque las soluciones relativas a la CMBD son de alcance estrictamente local; además, la interoperabilidad constituye una cualidad cuya complejidad excede la uniformidad del mensaje. Para graficar este punto, es necesario señalar que de poco serviría el

establecimiento de datos uniformes, pero estáticos o no integrados: el impulso debe ser idealmente holístico y parejo en todos los niveles que componen a la interoperabilidad.

Conviene destacar que la interoperabilidad significa libertad, en cuanto más información exista entre los sistemas informáticos clínicos, menor será la chance de que los pacientes queden capturados por un determinado proveedor. De este modo, los pacientes pueden elegir dónde atenderse, según sus necesidades y recomendaciones médicas.

Resulta necesario relevar que la tecnología puede facilitar los procesos asistenciales y de cuidado, aunque para esto es imprescindible que los funcionarios sean capaces de relacionarse adecuadamente con esta.

La ventaja de los estándares internacionales es que su implementación se lleva a cabo en formatos amables para el usuario, por ejemplo, el HL7 FHIR utiliza un servicio web RESTful API, mediante el que se pueden implementar todas las funciones CRUD (crear, leer, actualizar y borrar, por sus siglas en inglés). De todas maneras, será necesario capacitar a quienes los afecten aquellas brechas tecnológicas sustanciales propias de un país en el que la digitalización es la excepción.

Por otra parte, no hay que pasar por alto que todo CMBD debe almacenarse respetando las disposiciones y principios generales de la PDP, por ejemplo, diferenciando la información de carácter sensible de aquella que no lo es, tomando resguardos proporcionales según criticidad. Los estándares, al sistematizar y categorizar la información bajo criterios de eficiencia y calidad para el correcto funcionamiento del proceso asistencial, permiten abrir una instancia para protección de los DPS.

Actualmente nuestro sistema de salud presenta un grave problema: cuenta con registros de salud que llevan mucha información de manera precisa y ordenada, pero sin que estén unificados. La siguiente tabla muestra algunos de los registros no interoperables:

REGISTRO NO INTEGRADO	FUNCIÓN
Ley Ricarte Soto	Solicitar evaluación de financiamiento de medicamentos y dispositivos de alto costo por Ley Ricarte Soto (médico solicita).
Registro de Urgencia Vital que, además, es GES	Registrar que el paciente con Urgencia Vital tiene una patología GES.
Registro Nacional de Inmunizaciones	Registrar las inmunizaciones del Programa Nacional de Inmunizaciones (PNI) y de campaña.
Registro Nacional del Cáncer (RNC)	Notificar un cáncer, su estadio y tratamiento (registran oncólogos, anatomía patológica).

Sistema de Gestión de Garantías Explícitas de Salud (SIGGES)	Registrar a un paciente en el ingreso al GES para gestionar el cumplimiento de las garantías (registra equipo GES).
Sistema de Notificación de Eventos Supuestamente Atribuibles a Vacunación e Inmunización (ESAVI)	Notificar eventos supuestamente atribuibles a una vacuna. Registran profesionales de vacunatorios (principalmente Enfermería).
Sistema de Registro de Animales Mordedores (SIRAM)	Busca reducir el riesgo de brote de rabia en el país mediante un registro que permita establecer un vínculo dueño-mascota y conocer el estado sanitario de los animales. Registra profesional de salud al atender a un paciente mordido por animales.
Sistema de Toma de Muestras	Registrar la indicación (médico) de un examen de PCR COVID, registrar la toma de muestra (enfermería) y registrar el resultado de la PCR (laboratorio).
Sistema de Vigilancia Epidemiológica (EPIVIGILA)	Informar enfermedades de notificación obligatoria (ENO), médico notifica.
Sistema Nacional de Información Perinatal y Registro Nacional de Anomalías Congénitas (RENACH)	Registrar nacimientos y anomalías congénitas de Recién Nacidos (usuarios: matronas y obstetras).
Sistema Notificación de Reacciones Adversas a Medicamentos Red-RAM	Notificar reacciones adversas a medicamentos. Registran profesionales que identifican relación entre un efecto adverso y un medicamento (principalmente Químico-Farmacéuticos).
Sistema para Certificados de Unidad de Cuidados Paliativos para Beneficios Previsionales (Ley N°21.309)	Certificar paciente con enfermedad terminal para que pueda realizar retiro de fondos de la AFP (jefe de cuidados paliativos registra).
Sistema para Validación de Recetas Gráficas	Escanear receta retenida o receta cheque para digitalizarla (usuarios: médicos prescriptores y Químico-Farmacéuticos de farmacias que expenden).
Sistema RightNow de FONASA	Registrar información de pago de pacientes financiados mediante GRD. Subir Conjunto Mínimo Básico de Datos GRD (usuarios: equipos de facturación y de codificación).
Unidad de Gestión Centralizada de Camas (UGCC)	Registrar Urgencia Vital (médico de urgencia), solicitar derivación de paciente (médico - enfermería), registro diario de paciente hospitalizado por Covid y uso de recursos.
Sistema Integrado de Donación y Transplante (SIDOT)	Ingreso de pacientes a lista de espera de trasplante y registro de donación de órganos (médico o enfermera)
Sistema Nacional de Receta en Línea	Crear una receta o dispensar un fármaco en una farmacia (usuarios: médicos/odontólogos/matronas prescriptoras y farmacéuticos que despachan). Sistema cuenta con una API estándar de integración a registros clínicos que busca evitar la fragmentación y doble registro.

TABLA 8. ELABORACIÓN PROPIA EN BASE A POST DE ALEJANDRO MAURO EN FORO SALUD DIGITAL (2021). Disponible en: https://bit.ly/3zdXIT5. [consulta: 06 febrero 2022]

Los registros del sistema público de salud operan en paralelo a aquellos que, llevados por empresas del sector privado, son ofrecidos a distintos prestadores. Esto es relevante porque excepcionalmente algunas redes de salud, especialmente privadas, cuentan con interoperabilidad de fichas clínicas, manteniendo un acabado registro de las atenciones de salud efectuadas entre un mismo prestador y paciente a lo largo del país. Prueba de esto son los servicios de interoperabilidad para HCE que ofrecen tres empresas predominantes en esta área: Rayen Salud, InterSystem o Avis Latam. Esta última referencia entre sus

clientes al Servicio de Salud de Coquimbo, Arica y Valparaíso/San Antonio, sin mencionar cuál servicio específico han contratado. Asimismo, se adjudicó en 2018 la Gran Compra destinada a desarrollar la interoperabilidad de las fichas clínicas con ocasión de la implementación del programa Hospital Digital.[109]

Lamentablemente, el programa Hospital Digital desarrollado al alero de la Subsecretaría de Redes Asistenciales y que contemplaba el establecimiento de fichas clínicas electrónicas e interoperables, fue desfinanciado en 2020[110] , lo que se tradujo en que pasara de tener un presupuesto de $31.505.870.000 en 2019 a $5.130.000.000 en 2020.[111] [112] Dicha reducción se reforzó en el presupuesto 2021, alcanzando $4.700.883.000.[113] De ahí que las fichas clínicas electrónicas y la interoperabilidad no constituyan la regla general en el sistema de salud.

Respecto del mercado de las fichas clínicas electrónicas, la empresa Rayen Salud ofrece "el Servicio de Interoperabilidad de sistemas o softwares, que consolida distintas fuentes de datos y genera una Historia Clínica Compartida, entre diversos niveles de atención y/o Establecimientos de Salud, poniendo a disposición una visualización de registros de atención a través de un Portal Clínico". A pesar de que no existe información actualizada disponible, al año 2017 sus sistemas estaban disponibles en más de 650 centros de salud, involucrando más de 8.5 millones de fichas clínicas.[114]

Con pequeñas variaciones, la empresa InterSystem ofrece implementar la interoperabilidad bajo estándares de HL7 FHIR y reducir hasta en un 300% los costos de reingreso, asegurando que entre sus logros se encuentra la administración de más de 90 millones de fichas clínicas en EE.UU.[115]

---

[109] Recurso en línea: Gran Compra Nº 42.842, "Registro Clínico electrónico en modalidad de software como servicio (SAAS) para hospital digital". Disponible en: https://bit.ly/3wubhO7. [consulta: 06 febrero 2022]
[110] Recurso en línea: ¿Qué es Hospital Digital?. Disponible en: https://bit.ly/3qnzioO. [consulta: 06 febrero 2022]
[111] Recurso en línea: Ley de Presupuestos 2019, p. 643. Disponible en. https://bit.ly/3bUr3by. [consulta: 06 febrero 2022]
[112] Recurso en línea: Ley de Presupuestos 2020, p. 669. Disponible en: https://bit.ly/3BWvoWi. [consulta: 06 febrero 2022]
[113] Recurso en línea: Ley de Presupuestos año 2021 p. 699. Disponible en: https://bit.ly/3BWvoWi. [consulta: 06 febrero 2022]
[114] Recurso en línea: Interoperabilidad en Salud: El siguiente gran paso de la tecnología médica chilena. Disponible en: https://bit.ly/3mYnuHm. [consulta: 06 febrero 2022]
[115] Recurso en línea: Plataforma de interoperabilidad Intersystems HealthShare: Para organizaciones prestadoras de servicios de salud, p. 2-4. Disponible en: https://bit.ly/303oNMR. [consulta: 06 febrero 2022]

Otro actor del mercado es Avis Latam, que ofrece una licencia de gestión de salud ambulatoria, entre cuyas características está la gestión de fichas clínicas interoperables bajo estándares HL7 con una licencia de doce meses de duración y sin que los centros de salud autogestionen la solución tecnológica —en otras palabras, quienes contraten estos servicios quedan atados a pagos anuales—.[116]

Resulta favorable que los privados reemplacen los espacios que el Estado no ha cubierto, como ocurre con la interoperabilidad de las fichas clínicas, en la medida en que sea momentáneo. Sin embargo, el gran inconveniente que surge de los servicios que los privados ofrecen a este respecto son los datos personales sensibles, dando cuenta de la precaria regulación existente. Lo anterior será tratado en el capítulo dedicado al abordaje de las fichas clínicas desde PDP.

A nivel internacional se está impulsando el *International Patient Summary* (IPS), que tiene como "objetivo identificar los datos clínicos requeridos para la generación del Resumen de Paciente Internacional, con enlaces de vocabulario asociados y conjuntos de valores para resumen de pacientes […] y construir un documento internacional y plantillas asociadas basadas en HL7 CDA R2".[117]

En la medida en que Chile no cuente con un uso extendido de fichas clínicas electrónicas e interoperables, no podrá hacerse parte de esta iniciativa de cooperación internacional y será imposible el traspaso de información transfronteriza utilizando estándares semejantes al CDA u otros. Tampoco se podrá llevar a cabo correctamente, porque no se satisfacen los criterios internacionales necesarios para realizar operaciones de transferencias transfronterizas de datos personales que impliquen una cantidad significativa de información, cuestión que será analizada en el capítulo III.

10.- CUENTA MÉDICA INTEROPERABLE.

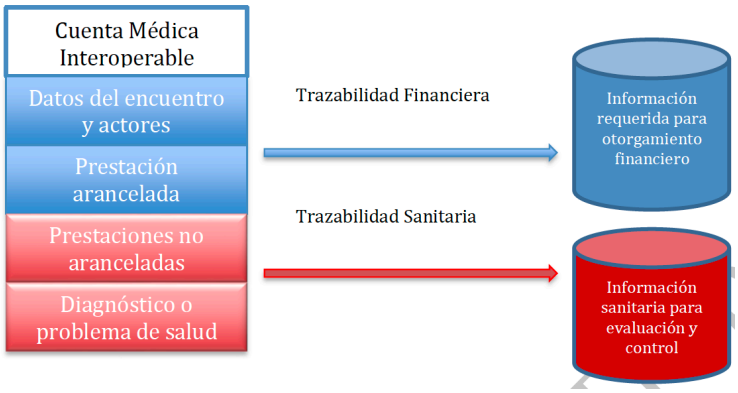
Un esfuerzo por implementar la interoperabilidad de las fichas clínicas lo constituyó la iniciativa CMI, anunciada el año 2017 por FONASA[118] y que se insertaba en la Agenda Digital 2020, cuyo capítulo 26 referido al "Sistema de Informatización de la Red Asistencial:

[116] Recurso en línea: Licencia de sistema de gestión de salud ambulatorio AVIS. Disponible en: https://bit.ly/3qk469W. [consulta: 06 febrero 2022]
[117] RACSEL. Manual estándares interoperabilidad en salud: Recomendaciones técnicas, 2019. p. 25.
[118] Recurso en línea: CENS — Cuenta Médica Interoperable. Disponible en: https://bit.ly/3odWCTp. [consulta: 06 febrero 2022]

Ficha médica electrónica", incluía como meta la "Implementación de plataforma de integración, que dé soporte a la interoperabilidad en la red de Servicios de Salud".[119]

La CMI consistía en una alianza pública-privada entre este organismo, el CENS y CORFO quienes, en coordinación con diversos prestadores implementarían una ficha clínica electrónica por paciente para el año 2020. El objetivo del programa era "que la información sanitaria y financiera necesaria para asegurar la continuidad del negocio entre los prestadores y el FONASA sea comunicada de manera interoperable y estandarizada, lo que finalmente se traducirá en un beneficio directo para los beneficiarios. El conocimiento que será posible generar de esta manera permitirá caracterizar el uso de los recursos, complementar y justificar la incorporación de nuevas prestaciones al sistema de financiamiento y así, eventualmente, mejorar la cobertura".[120]

Figura 5: Esquema proyecto de interoperabilidad



La CMI consideraba un beneficio potencial para 13 millones de personas, quienes podrían acceder directamente a las prestaciones disminuyendo los riesgos de diagnósticos errados o tratamientos incorrectos.[121]

La trazabilidad financiera resulta innovadora, porque el foco está puesto en lo sanitario, pero queda claro que no lo es todo. Según la exdirectora de FONASA, Dra. Jeanette Vega, "como ente asegurador público de salud, necesito saber qué le pasó a la persona, quién la atendió, y cuánto costó para poder darle protección financiera. El prestador, a su vez,

[119] Recurso en línea: Agenda Digital 2020 — Sistema de Informatización de la Red Asistencial: Ficha médica electrónica. Disponible en: https://bit.ly/3wu9eth. [consulta: 06 febrero 2022]
[120] Recurso en línea: Proyecto Cuenta Médica Interoperable, p. 11. Disponible en: https://bit.ly/3scZPq3. [consulta: 06 febrero 2022]
[121] Recurso en línea: CORFO — Fonasa, Corfo y CENS impulsan primer intercambio de información del paciente entre prestadores públicos y privados. Disponible en: https://bit.ly/304bnQM. [consulta: 06 febrero 2022]

requiere conocer mis reglas de protección financiera, para saber cuánto es el copago y cuánto le van a pagar".[122]

No existen antecedentes recientes sobre el desarrollo de esta iniciativa, por lo que podemos concluir que no llegó a prosperar; pareciera ser que un factor determinante para explicar la falta de implementación fue el cambio de gobierno, considerando que la CMI fue anunciada el año 2017, en el último periodo del segundo mandato de la presidenta Michelle Bachelet.

11.- DESGLOSE DEL ESTADO DE SITUACIÓN DE CHILE:

ÍTEM	ESTADO DE SITUACIÓN DE CHILE
Grado de aplicación de los estándares	- Bajo uso de estándar de mensajería HL7 v2. - Desarrollo de talleres de formación FHIR para evaluar uso en la historia clínica electrónica chilena. - Bajo uso de estándar de documentos clínicos CDA (principalmente para informes de alta, documentos clínicos y diagnósticos). - Amplio uso del estándar DICOM, especialmente para radiografía, tomografía o medicina nuclear. Se ha forzado el reconocimiento de este estándar para la transmisión de imágenes en todo Chile. Existe una disposición a nivel central para que todos los establecimientos que deseen comprar equipos radiológicos permitan la utilización del estándar. Los hospitales nuevos están obligados a partir con el estándar completamente incorporado (privacidad por diseño).
Grado de utilización perfiles IHE	- Se utilizan poco las guías IHE, lo que repercute en la falta de homogenización del lenguaje interoperable y la falta de aplicación de los perfiles IHE (es decir, el uso recomendado de estándares HL7 V2 y CDA).
Uso de OIDs	- No utiliza: al no estar codificada la información, esa se torna difusa, pierde calidad y tampoco se puede trazar inequívocamente su tratamiento.
Estado actual de los sistemas HIS en el país	- Parcialmente favorable. - Gracias a estrategia de informatización de los servicios de salud (Sistemas de Información de Red Asistencial o "SIDRA"), se coordina desde el nivel central la entrega de recursos. - Existen 29 servicios de salud y administran todos los hospitales públicos y algunos centros ambulatorio: un total de 1294 establecimientos de salud. Algunos de estos centros han optado por comprar una solución comercial y otros por el desarrollo propio. Cualquiera sea la opción elegida, es recomendable un plan de certificación para garantizar la interoperabilidad. - La cobertura de SIDRA a agosto 2015 era de 82%. - A septiembre de 2016, según una encuesta SIDRA, los tipos de procesos de centros sanitarios que están más avanzados en su informatización son agenda (91,6%), referencia-contrareferencia (94,8%), atención clínica ambulatoria (75,7%) y urgencias (63,7%).
Calidad de conexión	- Dispone de una buena calidad de conexión. Chile cuenta con una red privada para el sistema de salud público donde todos los centros que manejan fichas clínicas están conectados actualmente.

[122] Recurso en línea: Diario Financiero, Portafolio de Salud. Noviembre 2017 N° 29, p. 4. Disponible en: https://bit.ly/3bQcWE0. [consulta: 06 febrero 2022]

	REDMINSAL dota de conectividad a todos los centros de salud; en los sistemas de ficha clínica hay desorden. Existe un sistema predominante y otros menores, todos agrupados en estrategia sidra.
Centros con conexión a internet	Actualmente, la mayoría de los centros disponen de conexión a Internet. Todavía están pendientes las postas rurales pues no todas cuentan con conexión para transmisión de datos, aunque existen proyectos que tienen tal objeto.
Grado utilización de Servicios Web	Alto; en consecuencia, solo en algunas postas rurales sería recomendable formar a técnicos en el uso de esta tecnología.

TABLA 9. ELABORACIÓN PROPIA EN BASE A RACSEL (2019).

12.- DESARROLLO A NIVEL COMPARADO DE LA INTEROPERABILIDAD DE LAS FICHAS CLÍNICAS.

A. AUSTRALIA.

La importancia que Australia le otorga a las TIC de salud se manifiesta en la existencia de la *Australian Digital Health Agency*, entre cuyas funciones contempla "contribuir al desarrollo, monitoreo y gestión de especificaciones y normas para maximizar la interoperabilidad efectiva de los sistemas de salud digital en los sectores público y privado" (la traducción es nuestra).[123] Tiene la misión de generar estadística acerca del estado de situación de la salud digital: a junio de 2021, existen 21.02 millones de fichas clínicas electrónicas: un 91% del total.[124] Asimismo, cuentan con información en tiempo real sobre la cantidad de documentos (fichas, exámenes o financieros), los más vistos por los usuarios, la cantidad de personas que ha otorgado acceso amplio a su información médica, entre otros.

Además, destaca la *National Clinical Terminology Service* (NCTS), una unidad dependiente de la Agencia, "responsable de administrar, desarrollar y distribuir terminologías clínicas nacionales y herramientas y servicios relacionados para apoyar los requisitos de salud digital de la comunidad sanitaria australiana" (la traducción es nuestra).[125] Esto implica la publicación mensual de los últimos estándares, así como asistencia a los servicios de salud en el manejo personalizado de estos.[126] [127] Destaca la masificación en el uso del SNOMED-

[123] Recurso en línea: *Interoperability reports.* Disponible en: https://bit.ly/3oaDQfx. [consulta: 06 febrero 2022]
[124] Recurso en línea: *My Health Record* — Statistics and Insights, June 2021, p. 2. Disponible en: https://bit.ly/3klvlNw. [consulta: 06 febrero 2022]
[125] Recurso en línea: *National Clinical Terminology Service*. Disponible en: https://bit.ly/3H5Msgj. [consulta: 06 febrero 2022]
[126] Recurso en línea: Actualizaciones recientes de los estándares del NCTS. Información disponible en: https://bit.ly/304yNEW. [consulta: 06 febrero 2022]
[127] Recurso en línea: Herramientas del NTCS. Disponible en: https://bit.ly/3o9xr4r. [consulta: 06 febrero 2022]

AU, esto es, la derivación australiana del estándar SNOMED, que incluye "más de 350.000 conceptos activos con significados únicos y definiciones formales basadas en la lógica, organizados en jerarquías con múltiples niveles de granularidad. Estas jerarquías incluyen hallazgos clínicos, procedimientos, observables, estructuras corporales, organismos, sustancias y productos farmacéuticos/biológicos" (la traducción es nuestra).[128]

Lo propio ocurre con la AMT, la Terminología Australiana de Medicamentos.[129] Sin embargo, no existe constancia de la obligación de usar otros estándares para niveles de interoperabilidad distintos al semántico. De ahí que la labor de la NCTS todavía sea perfectible.

La Agencia tiene la facultad de contratar informes a terceros especializados en salud digital de modo que la interoperabilidad se potencie de conformidad a la evidencia.[130] Recientemente se emitió uno del experto en salud digital de la OMS, David Rowlands, quien recomendó la creación de una "*Health Interoperability Standards Office*" que normalizara los estándares internacionales para el sector sanitario australiano.[131] Además, se pidió que fuese capaz de medir el éxito de las iniciativas de normalización de interoperabilidad y la supervisión del modelo de gobernanza en esta área.[132] Esto último lo consideramos fundamental para el éxito de Chile con relación a la FCEI.

B. CANADÁ.

En Canadá, el desarrollo de la salud digital y adopción de estándares a nivel nacional se encuentra canalizado, desde el año 2000, por *Canada Health Infoway,* organización independiente sin fines de lucro.[133] Sus inversiones en iniciativas de salud digital han superado los 43.000 millones de dólares en beneficios, incluyendo 7.400 millones de dólares para el periodo 2020-2021.[134] El mérito de esta ONG es que centraliza todos los estándares utilizados en el país: *Canadian Clinical Data Set* (terminología común para recetas electrónicas); DICOM; HL7 FHIR; HL7 V3, CDA; IHE; ISO/TC 215 *Health*

[128] Recurso en línea: SNOMED CT-AU. Disponible en: https://bit.ly/30bSo6z. [consulta: 06 febrero 2022]
[129] Op. Cit.
[130] Recurso en línea: *Interoperability reports*. Disponible en: https://bit.ly/3oaDQfx. [consulta: 06 febrero 2022]
[131] ROWLANDS, David. A Health Interoperability Standards Development, Maintenance and Management Model for Australia, 2020. p. 120.
[132] Op. Cit.
[133] Recurso en línea: *Our history Canada Health Infoway*. Disponible en: https://bit.ly/305XQYd. [consulta: 06 febrero 2022]
[134] Op. Cit.

Informatics; *Nursing Data Standards*; LOINC; *Primary Health Care Electronic Medical Record Minimum Data Set* (PHC EMR MDS) y SNOMED CT CA/ SNOMED CT.[135]

Adicionalmente, *Canada Health Infoway* se encarga de precisar los estándares recomendados, así como las organizaciones con competencia para definirlos a nivel provincial.[136]

Por otro lado, en British Columbia, la página web de la provincia cuenta con un catálogo específico relativo a las normas de información de salud e interoperabilidad, que tienen por objeto implementar e integrar los sistemas de información clínica, las historias clínicas electrónicas, la terminología de los servicios locales y la arquitectura de los intercambios de documentos clínicos.[137] Cada estándar tiene información clara respecto de su estado actual, existiendo cuatro opciones: obsoleto, publicado, pendiente (su aprobación por el *Health Information Standards Standing Committee*, líder en "gobernanza de estándares") o en etapa de desarrollo.[138]

Por último, los estándares se encuentran segmentados según los sistemas de información clínica (*PharmaNet*, por ejemplo, utilizado para el intercambio de información entre servicios de salud y las farmacias), terminología (SNOMED CT o LOINC), arquitectura de documentos clínicos (CDA), FHIR (HL7 FHIR) o datos propiamente tal (*Conceptual Information Model* o CIM, un estándar utilizado para definir qué información de la persona es la que conforma la historia clínica electrónica y cómo es estructurada la información de salud).[139]

C. ESPAÑA.

El caso español destaca por replicar a nivel interno la regulación comunitaria. En esta línea, cuenta con una ley de interoperabilidad para toda la administración electrónica, en que se sistematizan los principios básicos del Esquema Nacional de Interoperabilidad y la

[135] Recurso en línea: *Canadian Standards*. Disponible en: https://bit.ly/3qp3DUd. [consulta: 06 febrero 2022]
[136] Recurso en línea: *Standards in Canada*. Disponible en: https://bit.ly/3FdaQLh. [consulta: 06 febrero 2022]
[137] Recurso en línea: *Health Information and Interoperability Standards Catalogue in British Columbia*. Disponible en: https://bit.ly/3BYi43E. [consulta: 06 febrero 2022]
[138] Recurso en línea: *Standards Status*. Disponible en: https://bit.ly/3BYi43E. [consulta: 06 febrero 2022]
[139] Op. Cit.

regulación común relativa a los niveles de interoperabilidad organizativa, semántica y técnica.[140]

Dentro del Esquema Nacional de Interoperabilidad existe el Centro de Interoperabilidad Semántica, cuya tarea es "publicar los modelos de datos de los elementos de interoperabilidad que permiten intercambiar información entre las Administraciones Públicas y entre éstas y los ciudadanos".[141] Asimismo, existe el Servicio de Interoperabilidad del Sistema Nacional de Salud, cuya misión es "establecer unos servicios de acceso de los profesionales sanitarios a la Historia Clínica Digital (HCD) del paciente desde cualquier punto del sistema", así como "ofrecer a los ciudadanos el acceso en línea a su historia clínica digital desde cualquier ubicación, por medio del DNI electrónico u otro certificado digital".[142]

Bajo el alero de este Servicio se ha desarrollado el proyecto de "Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS), que tiene como finalidad garantizar a ciudadanos y profesionales sanitarios el acceso a la documentación clínica más relevante para la atención sanitaria de cada paciente. [143] Asimismo, busca dotar al Sistema Nacional de Salud de un método seguro de acceso que garantice al ciudadano la confidencialidad de los datos de carácter personal relativos a su salud".[144]

La política de estándares para cada nivel de interoperabilidad constituye un eje fundamental de este proyecto, por lo que destaca en este documento el uso de XML para el intercambio de datos (interoperabilidad técnica), el HL7 CDA para el de información clínica (interoperabilidad sintáctica) y el DICOM para el de imágenes clínicas.[145]

Respecto de la interoperabilidad semántica, el Sistema Nacional de Salud utiliza OIDs, para que no exista ambigüedad cuando tenga lugar la comunicación transfronteriza.[146] Para esto,

---

[140] Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.
[141] Recurso en línea: Centro de Interoperabilidad Semántica. Disponible en: https://bit.ly/3qiAz0p. [consulta: 06 febrero 2022]
[142] Recurso en línea: Servicios de interoperabilidad del Sistema Nacional de Salud. Disponible en: https://bit.ly/3H6MlRm. [consulta: 06 febrero 2022]
[143] Recurso en línea: Instituto de Información Sanitaria. El sistema de historia clínica digital del SNS, 2009. p. 10. Disponible en: https://bit.ly/3BVi2tm. [consulta: 06 febrero 2022]
[144] Op. Cit.
[145] Recurso en línea: Grupo de Estándares y requerimientos técnicos (GERT). Política de estándares y normalización de datos, 2008. Disponible en: https://bit.ly/3bQJI7R. [consulta: 06 febrero 2022]
[146] Recurso en línea: Identificadores Únicos de Objetos (OID). Disponible en: https://bit.ly/2YvCDqs. [consulta: 06 febrero 2022]

ha desarrollado un catálogo de OIDs.[147] No obstante, la principal terminología clínica de referencia seleccionada para la HCDSNS corresponde al SNOMED CT.[148]

D. URUGUAY.

En América Latina destaca el caso uruguayo puesto que se han erigido como líderes en gobierno digital, ubicándose detrás de EE.UU. en la última encuesta ONU.[149] Al respecto, el trabajo de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), dependiente de la Presidencia de la República, tiene mucha influencia, pues ha impulsado el programa "Salud.uy", que promueve el uso intensivo de las TIC en el sector salud.[150]

Salud.uy forma parte de la Plataforma Nacional de la Salud, que aplica toda la Plataforma de Interoperabilidad —que también impulsa la AGESIC—, tanto a nivel técnico como normativo, extendiéndola y especializándola para el área de la salud.[151] En Uruguay, tal como en Europa, se está desarrollando la interoperabilidad para todo el sector público, no tan solo al área de la salud.[152]

Uruguay ha potenciado las fichas clínicas electrónicas a nivel normativo mediante el Decreto Nº 242/017 "Relativo a los mecanismos de intercambio de información clínica con fines asistenciales a través del sistema de historia clínica electrónica nacional" y el Decreto N° 122/019 sobre "Reglamentación del art. 194 de la ley 19.670, referente a la incorporación de las instituciones de salud y a las personas al sistema de historia clínica electrónica nacional".[153] [154] Esto porque la ley Nº 18.335 de 2008, sobre Derechos y Obligaciones de Pacientes y Usuarios, facultó al Poder Ejecutivo a través del artículo 20 a determinar criterios uniformes mínimos obligatorios de las históricas clínicas electrónicas.

---

147 Recurso en línea: Catálogo de OIDs. Disponible en: https://bit.ly/3odn8vY. [consulta: 06 febrero 2022]
148 Recurso en línea: SNOMED CT y la Historia Clínica Digital del SNS. Disponible en: https://bit.ly/3GZFObr. [consulta: 06 febrero 2022]
149 ONU. Encuesta sobre E-Gobierno. Departamento de Asuntos Económicos y Sociales, Nueva York, 2020. p. 46.
150 Recurso en línea: Sobre el centro. Disponible en: https://bit.ly/309qOa0. [consulta: 06 febrero 2022]
151 Recurso en línea: Ecosistema de Salud en Uruguay. Disponible en: https://bit.ly/31JMr1i. [consulta: 06 febrero 2022]
152 Recurso en línea: Plataforma de Interoperabilidad. Disponible en: https://bit.ly/3H39MLz. [consulta: 06 febrero 2022]
153 Decreto Nº 242/017.
154 Decreto Nº 122/019.

En cuanto a interoperabilidad sintáctica, utilizan el *HL7 Clinical Document Architecture* (CDA) para el intercambio de documentos clínicos y el HL7 V2 y V2 para mensajería.[155] A nivel de semántico, usan el estándar *IHE Cross Enterprise Document Sharing* (XDS) y el SNOMED CT, sobre la base de la existencia de CMBD previamente definidos.[156] [157] Tal como sucede con Australia, los estándares no son oficiales para el Estado y tampoco están homogeneizados. Por esta razón, el Comité de Informática en Salud del Instituto Uruguayo de Normas Técnicas está desarrollando proyectos de norma para la interoperabilidad de sistemas y redes telesalud.[158] [159]

13.- SÍNTESIS DE LOS CAPÍTULOS I Y II.

Hemos revisado en profundidad la legislación para el derecho a la protección de la salud, de las fichas clínicas y de la interoperabilidad. Asimismo, hemos ahondado en el concepto de interoperabilidad y profundizado en sus distintos niveles respecto de la Administración del Estado y en específico para el sector salud. Además, hemos abordado las funciones de FCE, sus beneficios, principios (generales y puntuales para las FCEI), barreras, estándares, la importancia del CMDB y los intentos infructuosos de la autoridad en este ámbito que se ven reflejados en la CMI.

En este contexto, es posible constatar la necesidad de actualizar el marco jurídico sectorial de nuestro país, complementando, sistematizando y perfeccionando la regulación, estableciendo la interoperabilidad a nivel marco estatal, y enfocada a las fichas clínicas, para coadyuvar al mandato constitucional del Estado en el marco de las acciones y prestaciones que permitan garantizar la salud de las personas en todas las fases de su ciclo vital, con independencia del prestador que haya participado directamente de cada una de dichas acciones y prestaciones.

Asimismo, habrá de impulsarse políticas públicas que implementen los estándares disponibles en materia interoperabilidad de historias clínicas en sus cuatro niveles,

---

[155] Recurso en línea: Principales Estándares y Perfiles. Disponible en: https://bit.ly/3EWvIWW. [consulta: 06 febrero 2022]
[156] Op. Cit.
[157] Recurso en línea: Modelo unificado. Disponible en: https://bit.ly/3odcXYf. [consulta: 06 febrero 2022]
[158] Recurso en línea: Proyectos de norma del Comité de Informática en Salud. Disponible en: https://bit.ly/3mW1TQ5. [consulta: 06 febrero 2022]
[159] Los anteproyectos de normas técnicas corresponden a PU UNIT-ISO/TR 16056-2:2004 y PU UNIT-ISO/TR 16065-1:2004.

siguiendo la abundante evidencia científica que respalda la FCEI y en la forma en que está establecido en las jurisdicciones analizadas.

Para ello, deberá homogeneizarse el conjunto mínimo de datos — o al menos la HRP— y terminar con la fragmentación de los distintos registros informáticos a cargo del MINSAL.

Estos pasos son esenciales para que Chile pueda sostener que el bienestar del paciente es la piedra angular del proceso asistencial.

Conforme con lo anterior, en el capítulo final realizaremos diversas recomendaciones basadas en la evidencia de países y organizaciones internacionales líderes en la materia, las cuales invitan a desarrollar la interoperabilidad en todas las áreas que el Estado comprende —incluyendo la salud—, midiendo su madurez sectorial y centralizando en un organismo público la gobernanza de los estándares.

CAPÍTULO III. PROTECCIÓN DE DATOS PERSONALES DE LAS FICHAS CLÍNICAS.

Tal como observamos anteriormente, la PDP corresponde a un ámbito crucial para las fichas clínicas, pues estas constituyen información sensible de los pacientes en su calidad de titulares.

Para entender su importancia conviene apoyarnos en el profesor español Antonio Pérez Luño:

> "[La] proyección de los efectos del uso de la informática sobre la identidad y dignidad humanas, incide también en el disfrute de los valores de la libertad y la igualdad. La libertad, en las sociedades más avanzadas, se halla acechada por el empleo de técnicas informáticas de control individual y colectivo que comprometen o erosionan gravemente su práctica. Contemporáneamente se produce una agresión a la igualdad, más implacable que en cualquier otro período histórico, desde el momento en que se desarrolla una profunda disparidad entre quienes poseen, o tiene acceso, al poder informático y quienes se hallan marginados de su disfrute.".[160]

En términos sencillos, "Internet ha abierto nuevas y preocupantes posibilidades operativas a los sistemas de control social y político".[161]

Estos planteamientos y sus riesgos han sido sintetizados por la Alta Comisionada de DD.HH. de las Naciones Unidas de la siguiente manera:

> "La tecnología digital se usa actualmente no solo para monitorear y clasificar, sino también para influir. Nuestros datos no solo se digitalizan, sino además se usan con fines mercantiles y políticos. El extremo oscuro del espectro digital amenaza no solo la intimidad y la seguridad personal, sino que además socava las elecciones libres y equitativas, hace peligrar la libertad de expresión, información, pensamiento y creencia, y sepulta la verdad bajo un alud de noticias falsas o *fake news*".[162]

En este orden de ideas, el CDH ha "reafirma[do] el derecho a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su

[160] PÉREZ LUÑO, Antonio. Los derechos humanos hoy: perspectivas y retos. XXII Conferencias Aranguren. Revista de Filosofía Moral y Política, Nº 51, 2014. p. 477.
[161] Op. Cit. p. 526.
[162] BACHELET, Michelle. Derechos humanos en la era digital: ¿Pueden marcar la diferencia? Discurso Alta Comisionada Derechos Humanos UN. Japan Society, Nueva York.

domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias establecidos en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.”.[163]

Sin embargo, las advertencias versan sobre de los datos de salud y los riesgos que su tratamiento conlleva. Basta imaginarse las posibilidades nocivas que surgirían en caso de que la industria farmacológica o sanitaria tomara control de una gran cantidad de información de salud de la población para cobros diferenciados y más altos según las necesidades de cada persona, lo que podría replicarse respecto de las altas autoridades del país, en el supuesto de que terceros o gran parte de la sociedad conocieran el diagnóstico médico de estas.

La misión del derecho público es regular la protección de los datos personales mediante el establecimiento de «límites» y «restricciones».[164] Los primeros, para que no se vulnere la intimidad de las personas cuyos datos se procesan y, las segundas, para que únicamente se usen los datos personales dentro de la competencia exclusiva de servicios públicos y para fines específicos.[165]

Estos límites y restricciones resultan indispensables para que el tratamiento de datos de salud no atente contra los derechos fundamentales de las personas. La PDPS constituye una condición necesaria para el ejercicio de otros derechos fundamentales, como el derecho a la identidad, a la intimidad y a participar en la vida económica y social, por lo tanto, su tratamiento puede dar cabida a nuevas formas de discriminación en el ámbito laboral, de salud y financiero.[166]

Ello explica el esfuerzo mancomunado y prematuro de Europa para dar lugar al primer instrumento internacional destinado a afrontar los desafíos que el incipiente tratamiento automatizado de datos personales representaba para los derechos de las personas, cuestión que ocurriría en Estrasburgo el año 1981. Dicha iniciativa se denominó “Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de

[163] CDH. El derecho a la privacidad en la era digital. Resolución aprobada por el Consejo de Derechos Humanos ONU el 7 de Octubre de 2021, Nº 48/4. p. 4.
[164] JIJENA, Renato. Tratamiento de datos personales en el Estado y acceso a la información, Revista Chilena de Derecho y Tecnología, Vol. 2, Núm. 2, 2013. p. 52.
[165] Op. Cit.
[166] BORDACHAR, Michelle. Los datos de salud en el proyecto de ley de protección de datos personales. El Mercurio Legal edición de fecha 4 octubre de 2019.

carácter personal", comúnmente conocido como Convenio 108, el cual ha sido ratificado por 55 países, siendo Uruguay el primer país latinoamericano en hacerlo el año 2013 —posteriormente se han sumado México (2018) y Argentina (2019)—. En lo medular, según su artículo 1º, el Convenio tiene por objeto asegurar en el territorio de cada Estado Parte a toda persona, cualquiera sea la nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales con respecto al tratamiento automatizado de datos personales. Además, con el paso del tiempo se ha ido actualizado para adecuarse a los avances tecnológicos, por ejemplo, la más reciente fueron las directrices publicadas sobre Inteligencia Artificial y PDP.[167] Lamentablemente, Chile se resta de esta colaboración internacional al no haber suscrito y ratificado el Convenio 108 y sus protocolos.

Sin perjuicio de lo anterior, un hito trascendental para el establecimiento de «límites» y «restricciones» fue la publicación el año 2018 de la ley Nº 21.096 que consagra la PDP como garantía fundamental autónoma en el artículo 19 Nº 4 de la Constitución Política de la República, porque cambió radicalmente el paradigma. Comparativamente, intentamos igualar la consagración constitucional que Uruguay logró en 1967, Colombia en 1991, Argentina en 1994 y Ecuador en 2008.

Hasta antes de 2018, los operadores jurídicos —tribunales de primera instancia conociendo acciones indemnizatorias o *habeas datas* y magistrados de Corte de Apelaciones a propósito de recursos de protección—, "deducían sus prerrogativas en base a un concepto amplio del derecho de propiedad, partiendo de la libertad de expresión, o del derecho a la intimidad de las personas y sus familias, como consecuencia de la falta de una formulación autónoma que sea plenamente funcional".[168] La reforma constitucional no se inclinó por una concepción económica de la PDP al modo en que sí lo hizo la LPVP, que privilegió la regulación de la industria antes que la capacidad de control de los ciudadanos sobre su información personal.

La historia fidedigna de la LPVP corrobora que ello sería advertido por el profesor Renato Jijena "quien propugnó la creación de una institución especializada que se encargue de la tutela de la intimidad y permita, en ese sentido, la restauración de los derechos conculcados y la aplicación consiguiente de las sanciones tales como multas, cancelaciones,

[167] Recurso en línea: *New Guidelines on Artificial Intelligence and Data Protection*. Disponible en: https://bit.ly/3LpgGNs. [consulta: 06 febrero 2022]

[168] Primer informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado en el Proyecto de ley que "Consagra el derecho a protección de los datos personales." (Boletín Nº 9.384-07). p. 10-11.

eliminaciones del registro […] la omisión de tal organismo en la iniciativa legal podría significar que la parte dogmática de ella sólo fuera una mera declaración de principios".[169]

El pasar del tiempo confirmaría que todos los planteamientos del precitado académico se cumplirían. Décadas más tarde, el propio profesor Jijena indicaría que la LPVP "fue redactada con asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento de los parlamentarios que la impulsaron".[170]

En cambio, "la reforma constitucional descartó un modelo regulatorio de derechos de propiedad para reconocer la relación jurídica entre personas y sus datos personales. Al estructurar el derecho en base a una idea de autodeterminación informativa y autocontrol de la información personal, la relación jurídica de los individuos es de titularidad sobre los datos personales".[171] Esto se tradujo en la imposición de mandatos al legislador y a todos los órganos del Estado relativos a la protección de los datos personales[172]; y, en concordancia con los artículos 19 Nº 26 y 63 Nº 2 del texto constitucional, el legislador añadió una reserva general y especial, de manera que sea siempre una ley la que determine las «formas y condiciones» del «tratamiento y protección» de datos personales.[173]

Asimismo, su consagración favoreció la tutela judicial efectiva a través de la acción de protección, que faculta a los tribunales de justicia a adoptar una amplia gama de medidas para el restablecimiento del imperio del derecho.[174] Además, permite superar la indefensión producida por los problemas procedimentales del *habeas data* (requiere abogado, se tramita ante juzgados civiles, por nombrar algunos), al tiempo que su consagración explícita

[169] Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado en tercer trámite constitucional, en el Proyecto de ley que "Consagra el derecho a protección de los datos personales." (Boletín Nº 9.384-07). p. 21.
[170] JIJENA, Renato. Actualidad de la protección de datos personales en América Latina. El caso de Chile, 2010. p. 414. EN: Memorias del XIV Congreso Iberoamericano de Derecho e Informática. Monterrey: VV.AA.
[171] CONTRERAS, Pablo. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena, Estudios constitucionales Vol. 18, Núm. 2, Santiago, 2020. p. 115.
[172] CONTRERAS, Pablo y TRIGO, Pablo. Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. Revista Chilena de Derecho y Tecnología, Vol. 8, Núm. 1., 2019. p. 71.
[173] ÁLVAREZ, Daniel. La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. Revista Chilena de Derecho y Tecnología, Vol. 9. Núm. 1, 2020. p. 3.
[174] SCS Rol Nº 71.906-2020.

impide que existan dudas respecto del derecho fundamental cautelado por la acción de protección.

Recordemos que la autodeterminación informativa se concibe como el "control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas"[175]; involucra un ámbito distinto al de la privacidad que, a fines del siglo XIX, los profesores Brandeis y Warren describirían como "*right to be left alone*", noción que con el desarrollo tecnológico se encargaría de demostrar su insuficiencia.[176]

Siguiendo al profesor Murillo de la Cueva, la autodeterminación informativa concierne a un bien jurídico distinto al de la intimidad, como lo es "asegurar a las personas el control de la información —de los datos— que les es propia para ponerles al resguardo o, al menos, permitirles protegerse de los perjuicios derivados del uso por terceros, públicos o privados, de ese material".[177] Esto sería justamente el objeto de la reforma constitucional según la historia fidedigna de la ley: "consagrar constitucionalmente el derecho a la PDP, y el derecho a la autodeterminación informativa, esto es, la facultad de las personas a controlar sus datos personales".[178]

Los pormenores de esta garantía fundamental serían definidos en un PDL que patrocinaron los entonces integrantes de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, que sería refundido en un mensaje de la presidenta Bachelet.[179] Esto permitiría cumplir compromisos internacionales que Chile adquirió con la OCDE en 2010, en particular, en lo referente a adecuar la legislación interna a sus directrices.[180] El mensaje incluye entre sus objetivos "Dotar al país de una legislación moderna y flexible en materia de tratamiento de datos personales, que sea consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y

---

[175] MURILLO, Pablo. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad, 2009. p. 11-12. EN: Murillo de la Cueva, Pablo Lucas y Piñar Mañas, José Luis, El Derecho a la Autodeterminación Informativa, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

[176] BRANDEIS, Samuel y WARREN, Louis. El derecho a la intimidad, Edición de Benigno Pendás y Pilar Baselga, Madrid: Civitas,1995.

[177] MURILLO, Pablo. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad, 2009. p. 18. EN: Murillo de la Cueva, Pablo Lucas y Piñar Mañas, José Luis, El Derecho a la Autodeterminación Informativa, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

[178] Objeto del proyecto de ley que "Consagra el derecho a protección de los datos personales." (boletín Nº 9.384-07). p. 7.

[179] Boletín 11.092-07 de 17 enero de 2017, patrocinado por los H. Senadores Pedro Araya, Alfonso de Urresti, Alberto Espina, Felipe Harboe y Hernán Larraín.

[180] Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales, 2002.

estándares internacionales".[181] Sin embargo, debido a que todavía el PDLPDP no logra sortear el primer trámite constitucional, la OCDE ha llegado a advertir a Chile en cuanto al cumplimiento de sus compromisos.[182]

La dilación legislativa se traduce en que la ley marco de PDP aplicable a las fichas clínicas siga siendo la LPVP de 1999, cuya técnica legislativa replica el modelo imperante en Europa hacia fines de los años noventa[183]: un cuerpo legal de carácter general o ley marco, al que se remite toda la legislación sectorial para reglar el tratamiento de datos que se produce con motivo de un contrato de trabajo, del seguro de desempleo, prestaciones de salud, entre otros.[184]

Este esquema regulatorio resulta insuficiente para la protección de las personas en el ámbito de su información de salud, por cuanto la LPVP no define específicamente los datos de salud, ni contiene una regulación sistemática de ellos, lo que se suma a las deficiencias estructurales de la ley, por ejemplo, en lo referente a la institucionalidad, régimen infraccional y protección de derechos de los titulares de datos.

La regulación se limita a que el tratamiento de fichas clínicas, por contener datos sensibles, esté prohibido salvo en tres casos: cuando una ley lo autorice; exista consentimiento del titular o que los datos sean necesarios para la determinación u otorgamiento de beneficios de salud. Sobre el particular nos remitimos a lo sostenido anteriormente en el título I.

Otras normas comunes aplicables a los datos de salud son la sujeción a la finalidad del tratamiento (incorporado por Ley Nº 20.635), la veracidad de la información (art. 6 y 9), deber de custodia (art. 11), seguridad (art. 5), temporalidad (art. 2 letra d) y 6 inciso primero), deber de secreto (art. 7), protección a los derechos del afectado (art. 12 y 16), tutela judicial vía *habeas data* ante los tribunales civiles (art. 16), principio de responsabilidad (art. 16 y 23), entre otros. Sin embargo, este esfuerzo es simbólico, por cuanto resulta evidente que la regulación general referida a los datos de salud no es proporcional a la trascendencia de los bienes jurídicos que protege, cuestión que ha quedado de manifiesto durante la pandemia de COVID-19. Esta desproporción ha motivado fuertes críticas doctrinarias,

[181] Mensaje Nº 001-365 del boletín Nº 11.144-07. p. 5.
[182] Recurso en línea: OCDE le pide a Chile avanzar en legislación de datos personales de aquí a diciembre. Disponible en: https://bit.ly/3BSmdpz. [consulta: 06 febrero 2022]
[183] CERDA, Alberto. Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, Núm. 3, 2003. p. 39.
[184] CERDA, Alberto. Legislación sobre protección de las personas frente al tratamiento de datos personales, Apuntes de clases, Centro de Estudios en Derecho Informático, 2012. p. 17.

incluso desde el inicio de la discusión legislativa de la LPVP, las que se han reforzado con el tiempo.[185]

Entre aquellos está el profesor Fabián Elorriaga, quien en el inicio de la tramitación de la LPVP apuntó a "la conveniencia de realizar una reflexión más profunda en lo relativo a la protección de los datos nominativos de las personas, orientada a pensar en un texto autónomo y mucho más completo, como ocurre en Francia, Suecia, Suiza, Islandia, Australia, Noruega, Irlanda, Japón, Alemania, Portugal Gran Bretaña y España.".

El profesor Alberto Cerda, hace casi diez años, alertó que no resultaba comprensible que la LPVP no estableciera al menos uno de los dos mecanismos de autocontrol consagrados a nivel comparado, sean estos códigos deontológicos o responsables internos de datos. Esto en el entendido de que "los principales interesados en el debido resguardo en el cumplimiento de la normativa sobre tratamiento de datos recaen en los propios interesados, en los sujetos que intervienen en el proceso, a saber, el responsable del registro o banco y los titulares de los datos personales".[186]

Recordemos que los códigos deontológicos son un "conjunto de preceptos que tipifican las infracciones y las sanciones relacionadas con el ejercicio de una determinada profesión"[187] y por tanto se enmarcan en los mecanismos de auto regulación.

Por su parte, los responsables internos —comisarios de datos—, se sustentan en la "*Bundesdatenschutzgesetz,* Ley Federal de Protección de Datos de la República Federal Alemana de 1977, en la que cada departamento administrativo o empresa privada que procesaba datos nominativos debía designar un comisario de protección dependiente de la entidad tratante, con formación profesional calificada, quien velaría por el cumplimiento de la ley sin quedar sujeto a instrucciones superiores para tal fin".[188] [189]

Asimismo, la LPVP presenta déficits de seguridad; en particular se le reprocha que sus exigencias no cumplan con los altos requerimientos que el desempeño de la actividad

[185] Primer Informe de la Comisión de Constitución del Senado en el proyecto de ley sobre "Protección de la vida privada" (boletín Nº 896-07). p. 5-6.
[186] CERDA, Alberto. Legislación sobre protección de las personas frente al tratamiento de datos personales, Apuntes de clases, Centro de Estudios en Derecho Informático, 2012. p. 39.
[187] Recurso en línea: Definición "código deontológico" RAE. Disponible en: https://bit.ly/3rWQemP. [consulta: 06 febrero 2022]
[188] CERDA, Alberto. Legislación sobre protección de las personas frente al tratamiento de datos personales, Apuntes de clases, Centro de Estudios en Derecho Informático, 2012. p. 40.
[189] Artículos § 28 y 29 del *Bundesdatenschutzgesetz* 1977.

sanitaria exige.[190] Sabemos que el personal médico requiere de altos estándares de seguridad para ejercer su profesión en el espacio físico, pero ¿qué explica que dichas exigencias no se repliquen en el ámbito virtual o en lo relativo al tratamiento de datos de salud? En ese entendido, resulta necesario implementar medidas que garanticen la autenticidad de las personas que acceden a los sistemas de tratamiento de datos de salud, junto con establecer un sistema de registro y trazabilidad y facilidades para que no se entorpezca el ejercicio de los derechos ARCOP.[191]

La doctrina, de forma unánime, considera que el principal defecto de la ley consiste en que los derechos consagrados no pasen de cumplir una mera función declarativa, a pesar de la enorme importancia que tiene la PDP para la vida de las personas.[192] [193] Esta situación es preocupante si se considera "la relación de manifiesto desequilibrio que por lo usual existe entre el titular de los datos y el responsable del tratamiento, lo que redunda en detrimento del primero".[194]

En este sentido, cuando se examina la historia fidedigna de la LPVP, "se podrá reparar en que los legisladores entendieron que estaban asumiendo en lo fundamental la normativa de europea, aun cuando progresivamente el énfasis estuvo en la impronta de la legislación española de 1992 […] pero a la hora de definirse por un órgano de control, el legislativo adscribió derechamente la doctrina norteamericana y optó por entregar la fiscalización en el cumplimiento de la normativa a las propias partes involucradas y no hacer intervenir al Estado, salvo en cuanto al rol que compete a los tribunales de justicia.".[195] Por lo demás,

[190] DONOSO, Lorena. El problema del tratamiento abusivo de los datos personales en salud, Expansiva, Santiago, 2011. p. 90.
[191] Op. Cit., p. 95-99.
[192] ÁLVAREZ, Daniel. Acceso a la información pública y protección de datos personales: ¿Puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?, RDUCN, Vol. 23. Núm. 1, 2016. p. 63.
[193] En cuanto al organismo al que se le dotará de competencia exclusiva en PDP, la discusión legislativa se ha variado entre el CPLT y una Agencia creada especialmente para estos efectos. Sin embargo, en septiembre de 2020, el Ejecutivo hizo público su cambio de parecer, anunciando que impulsaría una Agencia especializada, en desmedro del CPLT. Recurso en línea disponible en: https://bit.ly/3H20Rde. [consulta: 06 febrero 2022]
[194] CONTRERAS, Pablo y TRIGO, Pablo. Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. Revista Chilena de Derecho y Tecnología, Vol. 8, Núm. 1., 2019. p. 71.
[195] CERDA, Alberto. Intimidad de los trabajadores y tratamiento de datos personales por los empleadores. Revista Chilena de Derecho Informático, Núm. 2, 2003. p. 42-43.

España cambiaría su legislación poco tiempo después por efecto de la publicación en el año 1995 de la directiva comunitaria que antecede al GDPR (2016).[196] [197]

Ahora bien, el carácter declarativo de la LPVP obedece a la inexistencia de una autoridad capaz de "promocionar, proteger y promover los derechos establecidos en la LPVP, sino que también velar porque estos se respeten mediante el ejercicio o la amenaza del ejercicio de la potestad sancionatoria".[198] [199] Lo más grave es que estas deficiencias fueron advertidas durante la etapa prelegislativa a fines de los años noventa, por el exministro de Justicia, Francisco Cumplido. Años más tarde, Renato Jijena se encargaría de replicar en el tercer trámite constitucional ante el Senado.[200]

La inexistente o tenue institucionalidad se podría refutar señalando que desde 2008, con la publicación de la ley 20.285 sobre Acceso a la Información Pública, el CPLT cuenta con funciones en la materia. Por ejemplo, «velar por la debida reserva de los datos» y «velar por el adecuado cumplimiento de la LPVP por parte de los órganos de la Administración del Estado».[201] No obstante, esto resuelve solo una parte del problema, desde que el referido cuerpo normativo nada señala sobre el cumplimiento de la ley por parte de los particulares, lo que permite entender que "en la práctica la adopción de medidas de seguridad adecuadas y robustas para el tratamiento de datos personales no sea más que un acto cuasivoluntario cuya inobservancia no tiene consecuencias adversas o, las probabilidades de que ellas se materialicen son muy reducidas".[202]

A partir de este análisis, la profesora Lorena Donoso propone una "institucionalidad general y no fraccionaria; independiente y profesional, facultada para educar y formar a titulares de bancos de datos y sus mandatarios en el adecuado cumplimiento de la normativa y a los titulares de datos en el ejercicio de sus derechos; fiscalizar y sancionar las infracciones en

[196] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
[197] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
[198] ÁLVAREZ, Daniel. Acceso a la información pública y protección de datos personales: ¿Puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos?, RDUCN, Vol. 23. Núm. 1, 2016. p. 65.
[199] En igual sentido Jijena (2010, p. 414) y Donoso (2016, p. 27).
[200] CUMPLIDO, Francisco. Análisis del anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de Justicia (1990-1994), Ius et Praxis Vol. 3, Núm. 1, 1997. p. 201.
[201] Artículo 33 letras j) y m) ley Nº 20.285.
[202] BENUSSI, Carlo. Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes, Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 1, 2020. p. 244.

que se incurran; y colaborar y coordinarse con otros organismos similares a nivel comparado para adoptar criterios y soluciones armoniosas con las necesidades de cada momento".[203]

Una institucionalidad como la descrita permitiría equiparar las exigencias del GDPR (en particular las contenidas en el Capítulo IV, sobre Autoridades de Control Independientes) y satisfacer las exigencias de las directrices de la OCDE en lo relativo a que se brinden medios razonables para que los individuos ejerzan sus derechos y se sancionen adecuadamente las infracciones (Cuarta Parte de las Directrices OCDE 2002).

La regulación nacional vigente está incompleta en dos sentidos. Primero, por la ausencia de mecanismos de autocontrol como los códigos deontológicos o delegados internos de PDP, y, segundo, por contemplar únicamente el control jurisdiccional como mecanismo de heterocontrol, prescindiendo en gran medida de una autoridad de control administrativo. Así, podemos reconocer que las causas de ambas falencias confluyen en la inexistencia de una institucionalidad sectorial con potestades robustas y delimitadas sobre entidades del sector público y privado.

La precariedad de la legislación de PDP, y específicamente de DPS, desalienta la eventual implementación de FCEI puesto que los riesgos se podrían amplificar considerando que la información estaría obligada a circular, aunque sin un ecosistema jurídico-administrativo moderno que lo ampare.

Siguiendo a Donoso, "es así como la falta de regulación adecuada, sumada a la incapacidad del mercado de autorregularse, ha llevado a que en definitiva exista un tráfico de datos personales de salud que está afectando a sus titulares por distintas vías".[204] Por ello, resultaría aconsejable que el país esté dotado de una ley moderna de datos personales, previo a avanzar en el desarrollo de la interoperabilidad a nivel estatal y en el área de la salud. En este sentido, la aprobación del PDLPDP resulta indispensable.

Acerca de la desregulación y el tráfico de datos de salud, no podemos soslayar la ciberseguridad. De acuerdo con Deloitte (2021), la información de "una tarjeta de crédito tiene un valor comercial de pocos dólares en el mercado negro, mientras una ficha clínica

[203] DONOSO, Lorena. Protección de datos personales ¿Qué nos piden la OECD y la UE?, Revista del Colegio de Abogados de Chile, Núm. 66, 2016. p. 27.
[204] DONOSO, Lorena. El problema del tratamiento abusivo de los datos personales en salud, Expansiva, Santiago, 2011. p. 95.

puede llegar a costar en torno a los $100 dólares".[205] Este valor comercial permite entender las razones que justificarían un ataque *ransomware* a los hospitales Sótero del Río, La Florida, Padre Hurtado, San José de Maipo y CRS Cordillera "que significó una interrupción parcial del servicio que solo se pudo controlar después de varios días".[206] Según IBM, el sector salud es el que mayor costo incurre a nivel mundial por brechas de datos, alcanzando un promedio de $7.13 millones de dólares, que en el 50% de las veces se explica por ataques maliciosos.[207] Asimismo, es el sector que más tiempo promedio requiere para identificar y contener la brecha, con 329 días.[208]

En el caso del sector público estas brechas no son menores y más bien sí poseen un marco jurídico intimidante. En palabras de los profesores Jijena y Reveco:

> "[…] a propósito de la confidencialidad, entre otras varias normas jurídicas, la LOCBGAE establece la responsabilidad objetiva o por riesgo; el DS 83 obliga al resguardo de la información crítica basado en un enfoque de Gestión de Riesgos; la ley 19.799 permite la encriptación y la aplicación de diversas medidas técnicas para asegurar los efectos propios de la firma electrónica avanzada; además, por su parte, las leyes orgánicas propias de cada servicio u órgano de la administración del Estado establecen obligaciones de secreto tales como el secreto estadístico, el secreto tributario, la libre competencia, entre otros; las nuevas exigencias de seguridad y de ciberseguridad de la ley 19.880; la NCh oficial del INN publicó la ISO 27001-2013; la ley 19.628 hoy establece responsabilidades por el tratamiento de datos personales en el sector público; y existe obligación legal expresa de denunciar delitos a los Tribunales —bastante más eficaz como medida de contingencia que la obligación de notificar vulnerabilidades a los afectados— y se desconocen o se dejan de lado y no se operativizan.".[209]

1.- EJES DEL PDLPDP EN RELACIÓN CON LOS DPS.

Los beneficios del PDLPDP son sustantivos, por cuanto está inspirado en la regulación paradigmática a nivel mundial, como lo es el GDPR, destacando la presencia de la

[205] DELOITTE. La evolución de la ciberseguridad en el sector de la salud, Chile, 2021. p. 3.
[206] Op. Cit.
[207] IBM. Cost of a Data Breach Report, 2020. p. 12.
[208] Op. Cit.
[209] JIJENA, Renato y REVECO, Rodrigo. Ciberseguridad y responsabilidades en el sector público, Diario Constitucional, Artículos de Opinión, 2020.

Comisaria encargada de la Cartera de Justicia, Consumidores y Equidad de Género de la UE y vicepresidenta de la CE, Vera Jourová en el Congreso Nacional.

Los beneficios radican en el reconocimiento de las personas en cuanto titulares, estableciendo un título completo destinado a definir los derechos ARCOP y los principios, cuestión que es una deficiencia de la ley vigente; el PDLPDP es aún más ambicioso, considerando que incorpora el derecho a la inferencia —el derecho que tendría cualquier persona a conocer las valoraciones automatizadas de las que sean objeto—. Asimismo, destaca el hecho de que estos derechos sean ejercitables ante el responsable de los datos, a diferencia de lo que ocurre en la actualidad, puesto que se trata de una gestión judicial.

El segundo título contiene las reglas para el tratamiento de los datos personales y aborda las categorías especiales de datos. Resultan relevantes las exigencias establecidas para la formación del consentimiento, en cuanto este debe ser libre, informado y específico en relación con las finalidades del tratamiento. Además, su manifestación debe ser verbal, escrita o a través de un medio electrónico equivalente, aunque lo importante es que en cualquier caso sea inequívoco.

Cabe destacar que está contemplada una causal innovadora capaz de viciar el consentimiento, que se aparta de aquellas tradicionalmente contempladas en el Código Civil (error, fuerza, dolo). El PDLPDP pretende legislar el desequilibrio ostensible, que se verificaría en aquellos casos en que el consentimiento otorgado para la ejecución de un contrato o la prestación de un servicio no requieren del tratamiento de datos personales para su cumplimiento. Esto podría generar efectos significativos tratándose de prestaciones de salud y los potenciales alcances que tienen los datos tratados para esos efectos.

Otro elemento destacable para efectos de un adecuado tratamiento de fichas clínicas consiste en el deber de protección desde el diseño y por defecto, que, a nivel comparado está contenido en el artículo 25 del GDPR. En este sentido, todas aquellas entidades que traten DPS deberían contemplar medidas técnicas y organizativas apropiadas con anterioridad y durante el tratamiento de los datos para garantizar que se cumplan los principios y derechos que el proyecto establece. Una aplicación de interoperabilidad de fichas clínicas que en su etapa de desarrollo omita el ejercicio de los derechos de los pacientes estaría desde ya infringiendo la ley.

El deber de protección se ubica en una etapa causal distinta al anterior y apunta a contemplar medidas técnicas y organizativas de modo que solo se traten de los datos personales que sean necesarios para fines específicos y determinados del tratamiento. Por ejemplo, un proveedor de un servicio de salud podría acceder a datos de carácter estadístico para estimar la magnitud de los insumos, mas no a datos sensibles específicos y determinados, por cuanto no estaría ajustado a los fines derivados de su fuente de legitimidad.

Asimismo, recordando las críticas de Benussi sobre las medidas de seguridad en tanto "no serían más que un acto cuasivoluntario que no trae consecuencias adversas ante su inobservancia", el PDLPDP regula detalladamente dicho particular.[210] Las medidas de seguridad serán diferenciadas según el tipo de dato que se trate por la autoridad competente. Estas deben considerar el estado actual de la técnica y los costos de aplicación, junto con la naturaleza, alcance, contexto y fines del tratamiento, así como la probabilidad de riesgos y la gravedad de sus efectos en relación con el tipo de datos tratados.

Esta regulación ineludiblemente implicará que exista claridad en el ámbito de la salud respecto de las medidas de seguridad necesarias para resguardar esta clase de datos sensibles, lo que se contrapone a la libre iniciativa que propugna la autorregulación imperante, tal como sostuviera Donoso en 2011.[211] Esto se verá reforzado con la decisión de revertir la carga de la prueba cuando tengan lugar incidentes de seguridad, correspondiéndole al responsable del tratamiento acreditar la adopción de las medidas de adecuadas, siguiendo lo ya previsto en la ley N° 19.799, de firma y documento electrónico.

Quizás una de las mayores innovaciones para esta investigación sea la definición de datos relativos a la salud y al perfil biológico humano. A este respecto, el PDLPDP autoriza el tratamiento de estos con consentimiento previo del titular, para realizar diagnósticos, tratamientos médicos o mejorar la calidad y eficiencia de prestaciones de salud; prestar asistencia médica de urgencia; calificar el grado de dependencia o de discapacidad de una persona; o bien, cuando resulte indispensable para la ejecución o cumplimiento de un

[210] BENUSSI, Carlo. Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes, Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 1, 2020. p. 244.
[211] DONOSO, Lorena. El problema del tratamiento abusivo de los datos personales en salud, Expansiva, Santiago, 2011. p. 20.

contrato cuya finalidad lo exija. Además, permite el tratamiento de datos de salud y perfil biológico humano incluso sin consentimiento en los siguientes casos:

a. “Cuando este resulte indispensable para salvaguardar la vida o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento.
b. En casos de urgencia sanitaria legalmente decretada.
c. Cuando sean utilizados con fines históricos, estadísticos o científicos.
d. Cuando el tratamiento de los datos sea necesario para la formulación, ejercicio o defensa de un derecho ante los tribunales de justicia o un órgano administrativo.
e. Cuando el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de sistemas y servicios de asistencia sanitaria y social.
f. Cuando una ley lo autorice con indicación expresa de su finalidad.”

Adicionalmente, se prohíbe el tratamiento y la cesión de datos relativos a la salud y al perfil biológico de un titular y las muestras biológicas asociadas a una persona identificada o identificable, incluido el almacenamiento del material biológico, cuando los datos o muestras han sido recolectados en el ámbito laboral, educativo, deportivo, social, de seguros, de seguridad o identificación. Ello se traduce en el establecimiento de una cortapisa para prácticas asentadas en diversas industrias que acceden a datos de salud y que posteriormente utilizan para otros fines.

Muestra de ello es lo ocurrido en Codelco: los sindicatos de Chuquicamata denunciaron el acceso irregular a fichas clínicas de los trabajadores para tomar decisiones acerca de despidos.[212] Otro ejemplo serían los exámenes médicos que algunas instituciones bancarias exigen para otorgar créditos hipotecarios, cuestión que se sustenta en la recopilación de mejores antecedentes para evaluar el riesgo de una persona.[213] Lo anterior, a todas luces razonable, se transforma en abusivo cuando los resultados de los exámenes son negados a los propios titulares, quienes tampoco cuentan con mecanismos para

[212] Recurso en línea: BioBioChile — Dirigentes denuncian que Codelco accedió irregularmente a fichas médicas para iniciar despidos. Disponible en: https://bit.ly/3HdHcY2. [consulta: 06 febrero 2022]
[213] Recurso en línea: Diario El Mercurio edición 7 marzo 2021 — Esta es la lista de exámenes médicos que los bancos pueden pedir para comprar una casa. Disponible en: https://bit.ly/3BWtMfc. [consulta: 06 febrero 2022]

controlar su información personal. De ahí que no exista claridad respecto de los usos posteriores que las instituciones bancarias hacen con los exámenes médicos.

La fiscalización en el cumplimiento de la ley queda entregada a una institucionalidad con amplias competencias para el sector público y privado, y cuyo empoderamiento está dado por la imposición de multas gravosas con procedimiento expedito por la creación de un Registro Nacional de Sanciones y Cumplimiento, que no se trata solo de una hoja de vida, sino que quedan anotadas las entidades certificadas en sus respectivos modelos de prevención de infracciones. Estos pueden tener dos alternativas: la adopción de un encargado de prevención de PDP o la implementación de un programa de prevención de infracciones (comúnmente denominado *compliance*).

En el caso de la primera alternativa, los hospitales estarán obligados a tener claridad orgánica en el tratamiento de datos personales: a designar con nombre y apellido al responsable y al delegado, quien será el contacto con la autoridad competente.

En el caso de que implementen un programa de cumplimiento, estos deben contar con la designación de un delegado de PDP, la definición de sus medios y facultades, la existencia de mecanismos de reporte hacia autoridades y la obtención de certificación. Adicionalmente, el programa debe considerar, como mínimo:

1. Identificación del tipo de información tratada, el ámbito territorial en que opera, la clase de datos que administra y la caracterización de los titulares.
2. Identificación de las actividades habituales o esporádicas que aumenten el riesgo de cumplir infracciones a la ley.
3. Establecimiento de protocolos, reglas y procedimientos específicos para que las personas ejecuten sus labores con foco en la prevención de la comisión de infracciones.

Respecto de la institucionalidad, el presidente de la República hasta antes del 7 octubre de 2021 estuvo determinado a que el CPLT ampliara sus competencias hacia el ámbito de la PDP. Sin embargo, mediante el patrocinio de una indicación sustitutiva, rectificó su postura y sugirió la creación de un organismo nuevo, especializado y autónomo: APDP, lo que parece lógico puesto que la mayoría de los países OCDE se han inclinado por un sistema

unitario: Austria, Bélgica, Dinamarca, Franca, España, Finlandia, Francia, Grecia, Holanda, Irlanda, Islandia, Israel, Luxemburgo, entre otros.[214]

En este aspecto, las indicaciones resultan encomiables, pero no tanto la decisión de reemplazar el esquema sancionatorio de multas y sus reglas de determinación, las que, hasta antes de las indicaciones las infracciones se penalizarían de la siguiente manera:

INFRACCIÓN PDL	SANCIÓN
Infracciones Leves	Amonestación escrita o multa de 1 a 100 unidades tributarias mensuales (UTM).
Infracciones graves	Multa de 101 a 5.000 UTM.
Infracciones gravísimas	Multa de 5.001 a 10.000 UTM.

TABLA 10. ELABORACIÓN PROPIA EN BASE A PDLPDP.

Con las recientes indicaciones se elimina esta distinción tripartita y se contempla un tope de 10.000 UTM, cuyo monto exacto debe ser determinado por el Consejo Directivo de la APDP siguiendo ciertos criterios, por lo tanto, las reglas aprobadas fueron sustituidas íntegramente: si antes existían reglas puntuales para la ponderación de agravantes y atenuantes, ahora el procedimiento se restringirá a los criterios que el Consejo Directivo estime prudencialmente, tales como la gravedad de la conducta, número de afectados, beneficio económico reportado, capacidad económica del infractor, entre los que se encuentran las circunstancias modificatorias de responsabilidad.

La iniciativa, entonces, busca prevenir que las responsabilidades en que una persona natural o jurídica incurra, por esta ley, sean sin perjuicio de las responsabilidades civiles, penales o disciplinarias que les correspondan. De esta forma, se construye un robusto régimen sancionatorio distinto al existente en la ley, con el objetivo de lograr el cumplimiento formal y material de sus disposiciones.

No obstante, es necesario realizar ciertas advertencias. Primero, la disparidad de criterios aplicados para abordar los datos de salud en comparación con los de carácter económico, financiero, bancario o comercial, que están contenidos en un título específico de la ley; no es proporcional que datos sensibles no se incluyan en un título destinado a esos efectos, mientras que otros datos relevantes para el sector privado sí lo estén. Entendemos que esto obedece a razones legislativas, por cuanto las modificaciones al actual título III de la LPVP

[214] VERGARA, Gonzalo. Institucionalidad en protección de datos personales: Examen de variables regulatorias en el contexto de los proyectos de ley boletines 11.144-07 y 11.092-07 (refundidos). Informe solicitado por el H. Senador Kenneth Pugh, 2018. p. 7.

puedan tener por efecto sepultar la iniciativa, como ha ocurrido con los intentos para regular consolidación de deudas.

Estimamos que esta es una oportunidad para incluir la evaluación de impacto relativa a la PDP y consulta previa, establecido en la sección Nº 3, capítulo IV del GDPR, para promover un tratamiento especialmente prudente y diferenciado de los datos de salud. En virtud de dicha evaluación, "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales […]".[215]

Por su parte, de conformidad a la consulta previa, "el responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo […]".[216]

Por el volumen de datos sensibles que administra la salud pública, se recomienda garantizar que cualquier decisión que recaiga sobre la información personal obtenga un pronunciamiento de la autoridad especializada previamente, de forma que se ponderen los riesgos derivados de una operación de concentración societaria entre actores relevantes del sector salud.

En tercer lugar, el legislador debiera cautelar la independencia de la autoridad de datos personales —recordemos que la UE contempla esta característica en el artículo 8.3 de la Carta de Derechos Fundamentales—. Al respecto debe analizarse si el modelo propuesto en la indicación es suficiente para satisfacer los compromisos y estándares internacionales, sobre todo si tenemos presente que, en la propuesta, la APDP se relacionará con el presidente de la República —a través del MINECON—, organismo al cual se le atribuye la facultad de nombrar a los tres consejeros previa ratificación por los dos tercios de los miembros en ejercicio del Senado. Tal como ocurre en la CMF, la designación del presidente del Consejo Directivo de la APDP corresponderá a una prerrogativa del presidente de la República.

[215] Artículo 35 del GDPR.
[216] Artículo 36 del GDPR.

De ello desprendemos que la injerencia del Poder Ejecutivo sobre la futura APDP será sustantiva, lo que podría entorpecer la modernización de la LPVP en todos sus aspectos, incluyendo las características institucionales, además de comprometer su independencia.

En todo caso, advertimos diversos intentos de la autoridad por sortear la dilación legislativa del PDLPDP y la inexistencia de un organismo sectorial claro. Es así como, por la vía de indicaciones o PDLs, se ha propuesto proponer entregar competencias en estas materias a organismos existentes. Esto fue lo que ocurrió con el SERNAC con ocasión del PDL "Proconsumidor" que modificó la ley Nº 19.496 e incluyó un artículo 15 bis nuevo que otorgaba legitimación activa a este servicio para velar por el interés colectivo del consumidor frente a afectaciones en los datos personales de carácter económico.[217] Otro caso es el del PDL FINTECH, en tramitación, que de aprobarse ampliaría excesivamente las atribuciones que la CMF respecto de los datos de carácter financiero, por ejemplo, con el Sistema de Finanzas Abiertas.[218]Tanto el caso del SERNAC como de la CMF son una muestra de que la competencia de la futura APDP se está diluyendo entre distintos organismos, propiciado por la dilación legislativa del proyecto marco.

Estimamos que sería aconsejable concentrar en un solo organismo la competencia relativa a la PDP de modo que no existan conflictos entre entidades del sector público y no se abra la puerta a la confusión de la ciudadanía respecto de quién es el encargado de velar, fomentar y fiscalizar el respeto a sus derechos con los consiguientes problemas de certeza jurídica. Considerando la extensión del PDLPDP, estimamos conveniente ilustrar sus enmiendas e innovaciones con respecto a la LPVP a través de la siguiente tabla:

[217] PDL que "Establece medidas para incentivar la protección de los derechos de los consumidores" (boletín 12.409-03). Actual ley Nº 21.398.

[218] PDL que "Promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros" (boletín 14.750-05).

CONCEPTO	LPVP	PDLPDP
Datos Personales	✓	✓
Proceso de anonimización o disociación	✓	✓
Registro/Banco de datos/Base de datos personales	✓	
Responsable de tratamiento	✓	✓
Encargado/Intermediario de tratamiento		✓
Transferencia internacional de datos/tratamiento transfronterizo		✓
Consentimiento expreso y escrito	✓	
Consentimiento libre, informado y específico		✓
Fuente accesible al público	✓	✓
Interés legítimo		✓
Desequilibrio ostensible para exclusión del consentimiento como base jurídica del tratamiento		✓
Elaboración de perfiles		✓
Derecho de Acceso	✓	✓
Derecho de Rectificación	✓	✓
Derecho de Cancelación	✓	✓
Derecho de Oposición	✓	✓
Derecho de Portabilidad		✓
Derecho de Inferencia		✓
Registro Nacional de Cumplimiento y Sanciones		✓
Principio de Legalidad/Licitud	✓	✓
Principio de Finalidad	✓	✓
Principio de Calidad	✓	✓
Principio de Proporcionalidad		✓
Principio de Transparencia/Información	✓	✓
Principio de Responsabilidad	✓	✓
Principio de Confidencialidad	✓	✓
Principio de Seguridad	✓	✓
Deber de adoptar medidas de seguridad		✓
Deber de reportar vulneraciones a medidas de seguridad		✓
Diferenciación estándares de cumplimiento de obligaciones		✓
Datos sensibles	✓	✓
Datos personales relativos a la salud		✓
Datos personales biométricos		✓
Datos personales relativos al perfil biológico humano		✓
Datos personales relativos a niños, niñas y adolescentes		✓
Datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones		✓
Datos de geolocalización		✓
Big Data		✓
Autoridad de control administrativo		✓
Autoridad de control judicial	✓	
Procedimiento de reclamación judicial	✓	✓
Diferenciación entre infracciones leves, graves y gravísimas		✓
Sanciones de multas diferenciadas por naturaleza de la infracción		✓
Circunstancias agravantes y atenuantes		✓
Sanciones accesorias		✓
Responsabilidad civil	✓	✓
Modelos de prevención de infracciones		✓

TABLA 11. ELABORACIÓN PROPIA.

2.- EXPERIENCIA COMPARADA EN PROTECCIÓN DE DATOS PERSONALES DE SALUD.

A. AUSTRALIA.

Los principales cuerpos normativos de PDP son la *Privacy Act* de 1988 y los Principios Australianos de Privacidad, con aplicación general sin perjuicio de los cuerpos jurídicos locales. Esto se complementa con las normas de *My Health Record Act* de 2012.

A nivel institucional, la autoridad competente en datos personales corresponde a la *Office of the Australian Information Commissioner* (OAIC) de la que se desprende un Comisionado de Privacidad encargado de velar y fiscalizar el cumplimiento de la ley. En paralelo, existe la *Digital Health Agency* encargada de operar el sistema de *My Health Record* y el *Australian Cyber Security Centre (ACSC)*, aunque la primera también colabora en este aspecto en lo que específicamente le concierne.[219] [220]

En el sitio web de la OAIC destaca la existencia de guías interactivas disponibles para que las personas puedan ejercer eficazmente sus derechos relacionados con su información de salud y puedan operar el sistema *My Health Record*. Por ejemplo, existen guías prácticas para que las personas accedan a su información de salud y la corrijan y también existen otras de carácter informativo sobre los alcances del tratamiento de DPS y el sistema *My Health Record*.[221]

La página web de OAIC ofrece guías de buenas prácticas para que los proveedores de servicios de salud protejan adecuadamente los datos de salud; por ejemplo, para recolectar, dar acceso, corregir, revelar a terceros o utilizarlos con fines investigativos.[222] Asimismo, posee guías de buenas prácticas aplicables al reporte obligatorio de filtraciones de fichas clínicas que los proveedores de salud deben realizar a la OAIC y a la *Australian Digital Health Agency*.[223]

---

[219] Recurso en línea: *About us — Digital Health Agency*. Disponible en: https://bit.ly/3qjpix1. [consulta: 06 febrero 2022]
[220] Recurso en línea: *About the* ACSC. Disponible en: https://bit.ly/3wAw02M. [consulta: 06 febrero 2022]
[221] Recurso en línea: *Learn more about My Health Record*. Disponible en: https://bit.ly/3EOt3hU. [consulta: 06 febrero 2022]
[222] Recurso en línea: *Guide to health privacy*, September 2019. Disponible en: https://bit.ly/3yoQRa3. [consulta: 06 febrero 2022]
[223] Recurso en línea: *Guide to mandatory data breach notification in the My Health Record system*. 6 October 2017. Disponible en: https://bit.ly/3BSmWHj. [consulta: 06 febrero 2022]

Destacamos especialmente la guía de buenas prácticas para el cumplimiento adecuado de la *Rule* 42 de la *My Health Records Rule 2016*, puesto que acá se establecen las políticas de privacidad de los proveedores de salud. En virtud de esta norma, los proveedores están obligados a mantener, comunicar y promover el cumplimiento de su política de privacidad. Dicho documento, a su vez, debe contener la delimitación de accesos sobre el *My Health Record system* e incluir ciertas hipótesis de suspensión o desactivación de las autorizaciones internas; la capacitación previa a la que se someterá el personal, un procedimiento para identificar a quien solicite acceso de una ficha clínica e informarlo a la *Australian Digital Health Agency* en cuanto es la entidad que opera el sistema. Asimismo, incluirá medidas físicas y técnicas de ciberseguridad para proteger la información de salud y mecanismos expeditos para la identificación de incidentes y posterior implementación de medidas de mitigación.[224]

Según las buenas prácticas de la OAIC, conforme a la Rule 42, se recomienda a los proveedores de salud[225] que (i) recojan su política de privacidad en un único documento; (ii) contemplen un registro cronológico de todos los accesos de los empleados al *My Health Record system*, incluyendo la identidad tanto del trabajador que accede como del paciente cuya ficha clínica es consultada, además del día y hora en que se produjo, para que los accesos ilícitos puedan ser detectados; (iii) apliquen las recomendaciones de la *Australian Digital Health Agency* para que las contraseñas de los empleados que acceden al sistema tengan 13 o más caracteres (incluyendo letras, números y símbolos); (iv) implementen prácticas razonables para administrar las cuentas de los usuarios suspendiendo, por ejemplo, el acceso al sistema de un empleado que ingrese a pesar de que esté en conocimiento de que la seguridad de su cuenta o contraseña se ha visto comprometida; (v) llevar a cabo al menos una vez al año capacitaciones para todo el personal sobre los ámbitos de privacidad y seguridad de *My Health Record*, debiendo organizar otras acordes, según existan cambios en la legislación o funcionalidades del sistema.

El mismo Comisionado de Privacidad de la OAIC tiene la posibilidad de solicitar ante un tribunal la aplicación de una multa de hasta AUD$ 2.1 millones (EUR$ 1.3 millones) para personas jurídicas y de hasta AUD$ 420.000 para personas naturales ante un incumplimiento grave o reiterado de los principios de privacidad (la traducción es

[224] My Health Records Rule de 2016, Nº 42 Healthcare provider organization policies.
[225] Recurso en línea: *Rule 42 guidance OAIC*. Disponible en: https://bit.ly/3bPnSlo. [consulta: 06 febrero 2022]

nuestra).[226] Asimismo, tiene atribuciones para imponer compromisos ejecutables, conceder compensaciones/reembolsos y publicar determinaciones/decisiones públicas que especifiquen todos los detalles de la infracción —en caso de una denuncia— y los resultados de la investigación realizada.[227]

Por ejemplo, el 30 junio de 2021 —a propósito de la filtración de datos de cerca 1.2 millones de usuarios y conductores de Uber ocurrida en 2016—, la Comisionada de Privacidad determinó que para que la compañía se ajustara a los Principios de Privacidad Australianos debía garantizar la no repetición de los acontecimientos e implementar—en un plazo de doce meses— una política de recopilación y destrucción de datos, un programa de ciberseguridad que incluya a un coordinador interno y un plan de contingencia frente a brechas de seguridad, todo lo que debería ser certificado por expertos independientes (la traducción es nuestra).[228]

Por último, en vista de un bullado caso en materia de salud digital, no podemos dejar de mencionar al *Australian Competition and Consumer Commission* (ACCC) como una de las autoridades australianas que se encuentra velando por la privacidad de los pacientes, por más que su función corresponda a la libre competencia y los derechos del consumidor.[229] Nos referimos al caso de *HealthEngine*, una *start-up* que logró generar el mercado de salud en línea más grande de Australia basando su negocio en un repositorio digital compuesto por más 70.000 médicos y profesionales de la salud en Australia, donde los consumidores (pacientes) pueden gestionar sus reservas, además de publicar reseñas y calificaciones que sirvan de insumo para la elección de otros consumidores (la traducción es nuestra).[230]

En particular, HealthEngine admitió que entre el 30 de abril de 2014 y el 30 de junio de 2018 entregó información personal no clínica (nombres, fechas de nacimiento, números de teléfono, direcciones de correo electrónico) de más de 135.000 pacientes a corredoras de seguros de salud privadas, sin que los consumidores estuvieran en conocimiento y, en consecuencia, sin que estos hayan tenido la posibilidad de ejercer un control efectivo sobre

---

[226] Recurso en línea: *OneTrust Dataguidance. Australia – Data Protection Overview*. Disponible en: https://bit.ly/3keD1RK. [consulta: 06 febrero 2022]
[227] Op. Cit.
[228] Recurso en línea: *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy) [2021] AICmr 34 (30 June 2021)*. Disponible en: https://bit.ly/3oKaCpg. [consulta: 06 febrero 2022]
[229] Recurso en línea: *About the ACCC*. Disponible en: https://bit.ly/3bTkjur. [consulta: 06 febrero 2022]
[230] Recurso en línea: ACCC v HealthEngine Pty Ltd [2020] FCA 1203), p.1. Disponible en: https://bit.ly/3qnMGJB. [consulta: 06 febrero 2022]

su información, cuestión que les permitió generar cerca de AUD$ 1.8 millones.[231] Asimismo, admitió que "entre el 31 marzo 2015 y el 1 marzo 2018 no publicó cerca de 17.000 reseñas y editó otras de 3.000 para remover aspectos negativos o ensalzar los comentarios", provocando que los consumidores eligieran un prestador de salud que en otras circunstancias no hubiesen preferido.[232] Por estas infracciones, la compañía fue condenada al pago de AUD$ 2.9 millones en agosto de 2020.[233]

B. CANADÁ.

Este país no tiene una legislación marco, como en Europa o Chile, sino que la regulación de PDP se diferencia atendiendo el sector de que se trate. En esta línea, el sector público se rige por lo dispuesto en la *Privacy Act* de 1985, mientras que el sector privado se atañe a la *Personal Information Protection and Electronic Documents Act* (PIPEDA) de 2004. Esta regula el tratamiento de datos personales que realicen entidades privadas para atender fines comerciales, excepto en provincias o territorios en los que existan leyes "sustancialmente similares" a PIPEDA (la traducción es nuestra).[234]

Esta excepción a PIPEDA también se verifica respecto de Ontario, New Brunswick, Nueva Escocia o Terranova y Labrador, territorios que han adoptado regulaciones sustancialmente similares para el tratamiento de DPS.[235] Al respecto, destaca especialmente la de Ontario: la *Personal Health Information Protection Act* (PHIPA) que, de conformidad a su artículo 1º tiene por objeto establecer reglas, infracciones y mecanismos de tutela para el tratamiento de información personal de salud, con el propósito de velar por la confidencialidad de la información y la prestación efectiva de las atenciones médicas.

A escala federal, la autoridad de datos personales corresponde a la *Office of the Privacy Commissioner of Canada* (OPC).[236] Esta institución tiene competencia para velar por la *Privacy Act* y PIPEDA en todas las provincias y territorios, a excepción de British Columbia,

---

[231] Recurso en línea: *HealthEngine to pay $2.9 million for misleading reviews and patient referrals*. Disponible en: https://bit.ly/3odU3Au. [consulta: 06 febrero 2022]
[232] Op. Cit.
[233] Op. Cit.
[234] Recurso en línea: OPC 2020 — *Privacy Guide for Businesses*, p. 4. Disponible en: https://bit.ly/3wqYMTc. [consulta: 06 febrero 2022]
[235] Op. Cit.
[236] Recurso en línea: *About the OPC*. Disponible en: https://bit.ly/3EXoXEd. [consulta: 06 febrero 2022]

Alberta y Quebec.[237] Paralelamente, cada provincia y territorio tiene su propio *Privacy Commissioner*, quienes se encargan de velar por el cumplimiento de las normas referentes a la privacidad por parte del sector público, así como los estatutos locales que la regulan en el ámbito de la salud.[238]

En Ontario existe la *Information and Privacy Commissioner* (IPC), cuyo comisionado es un funcionario nombrado por la Asamblea Legislativa e independiente del gobierno de turno (la traducción es propia).[239] Esta entidad tiene la particularidad de reunir en un mismo organismo las competencias para velar por valores tan semejantes, pero tan distintos como la transparencia y la privacidad, cuestión que en Chile ha dado lugar a álgidas discusiones a propósito de establecer una institucionalidad con competencia exclusiva o compartida en la materia (en este último caso, sería el CPLT).

Asimismo, fuera de la institucionalidad que está encargada de velar por la PDP, es importante realzar la labor de *Health Canada*, que forma parte del gobierno federal y se encarga de la gobernanza de la industria alimentaria, cosmética, farmacéutica o de dispositivos médicos.[240] *Health Canada "*recibe información clínica para evaluar la seguridad y eficacia de los medicamentos y dispositivos médicos que se presentan para obtener su aprobación previo a su venta al público" (la traducción es nuestra).[241] Al tratar una magnitud considerable de información que luego es divulgada a terceros, resulta imprescindible regular ciertos procedimientos que garanticen el pleno respeto de la privacidad de la información de las personas involucradas, así como para llevar a cabo exitosas operaciones de anonimización. Para atender esta necesidad, ha publicado guías para la divulgación de información clínica.[242]

En razón a la organización territorial del Estado canadiense, caracterizada por la dispersión normativa y por el recelo a la instauración de autoridades con poder centralizado, la OPC

[237] Recurso en línea: *OneTrust Dataguidance. Canada – Health & Pharma Overview, June* 2021. p. 8. Disponible en: https://bit.ly/3goIgMu. [consulta: 06 febrero 2022]
[238] Op. Cit.
[239] Recurso en línea: *Role and Mandate of the Information and Privacy Commissioner of Ontario*. Disponible en: https://bit.ly/3F0OhJE. [consulta: 06 febrero 2022]
[240] Recurso en línea: *OneTrust Dataguidance. Canada – Health & Pharma Overview. June* 2021, p. 9. Disponible en: https://bit.ly/3goIgMu. [consulta: 06 febrero 2022]
[241] Recurso en línea: *Public Release of Clinical Information: guidance document.* Disponible en: https://bit.ly/3bQgAxG. [consulta: 06 febrero 2022]
[242] Op. cit.

se preocupa de orientar a los ciudadanos para que tengan claridad ante el organismo al que deben dirigir sus consultas relacionadas con sus datos de salud.[243]

En ejercicio de sus atribuciones para promover la PDP por la vía de la publicación de guías temáticas orientadoras para el sector público y privado, la OPC actualizó —en agosto de 2021— una serie de documentos para reforzar lo que PIPEDA concibe como información sensible, es decir, datos de salud que, en virtud de su naturaleza, requieren de la adopción de especiales resguardos.[244]

Cabe acotar que este esfuerzo de la OPC se explica en la obligación de revisión de las decisiones de adecuación para la realización de transferencias transfronterizas de datos personales que el GDPR en su artículo 45.3 exige realizar cada cuatro años a terceros países. En el caso de Canadá, desde 2001 se cataloga como un país "adecuado" por la UE.[245] Al mantener inamovible la decisión de adecuación, se subentiende que PIPEDA no colisiona con elementos básicos del GDPR, permitiendo que el flujo de información personal de sus ciudadanos ocurra con pleno respeto a sus derechos.

Esta armonía del GDPR con PIPEDA se verifica respecto de la legislación provincial o territorial, por cuanto esta debe ser compatible con los PIPEDA *fair information principles*, que forman las reglas básicas para la recopilación, uso y divulgación de información personal y dan a las personas control sobre cómo se manejan sus datos en el sector privado.[246] Se trata de diez principios que fueron sistematizados por el *Canadian Standards Association* en el año 1996 en base a un *Model Code* que tuvo como efecto que todas las organizaciones —incluyendo entidades a cargo de tratar datos de salud— deban respetarlos.[247] Entre estos principios están contemplados, por ejemplo, el consentimiento, finalidad, exactitud, acceso o *compliance*.[248]

---

[243] Recurso en línea: *Who to contact with concerns about the protection of your personal health information.* Disponible en: https://bit.ly/3oer0gx. [consulta: 06 febrero 2022]

[244] Recurso en línea: *OPC updates guidance regarding sensitive information, August 13, 2021*. Disponible en: https://bit.ly/3H62SF8. [consulta: 06 febrero 2022]

[245] Decisión 2002/2/CE de la Comisión de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.

[246] Recurso en línea: *Model Code for the Protection of Personal Information*. Disponible en: https://bit.ly/31NqWwJ. [consulta: 06 febrero 2022]

[247] Recurso en línea: *OneTrust Dataguidance. Canada – Health & Pharma Overview. June* 2021, p. 22. Disponible en: https://bit.ly/3goIgMu. [consulta: 06 febrero 2022]

[248] Recurso en línea: *PIPEDA fair information principles, May 2019*. Disponible en: https://bit.ly/3klshRL. [consulta: 06 febrero 2022]

Ahora bien, retomando la institucionalidad a escala provincial, destacamos al IPC de Ontario en cuanto es el organismo encargado de velar y fiscalizar las disposiciones de la *Personal Health Information Protection Act* (PHIPA), pero sobretodo por ser la entidad competente para publicar guías de buenas prácticas en relación con el tratamiento de datos de salud.[249] En contexto pandémico resulta destacable su guía referente a los aspectos de privacidad y seguridad en relación con las atenciones de salud virtuales.[250] Dicho documento precisa que el respeto de PHIPA aplica a todas las entidades tratantes de datos de salud, a través de medios físicos o digitales, debiendo velar por el principio de minimización, finalidad y seguridad.[251] Asimismo, recomienda adoptar una evaluación de impacto para las atenciones de salud virtual, una política de privacidad específica para estos fines, capacitaciones permanentes para los funcionarios involucrados, un marco de ciberseguridad robusto y un protocolo para gestionar brechas de seguridad que afecten a datos de salud.[252]

Destacamos también la guía para evitar el abandono de fichas clínicas producto de los cambios en la práctica médica y la incorporación de tecnología.[253] Esto porque, si bien en la Parte II de PHIPA están reguladas las prácticas para proteger la información personal de salud, esta guía enfatiza en la obligación que los custodios de datos de salud tienen antes, durante y después de los eventuales cambios que implementen en su práctica profesional.[254] En esta línea, el documento entrega recomendaciones puntuales para la gestión de fichas clínicas por parte de empresas de almacenaje a las que les corresponde acatar políticas de privacidad del custodio principal, respetar el principio de minimización, cobrar hasta el monto que PHIPA permite para acceder o divulgar el contenido de fichas clínicas y notificar oportunamente en caso de que ocurra una brecha de seguridad.[255]

Asimismo, la guía ofrece recomendaciones y contenidos mínimos en el aviso que los custodios de las fichas clínicas deben dar a los individuos afectados por el cambio en el ejercicio profesional indicando, por ejemplo, una vía de contacto, el tiempo en que serán

[249] Recurso en línea: Listado completo de las guías sobre buenas prácticas para el tratamiento de datos de salud IPC Ontario. Disponible en: https://bit.ly/3H2Vs5A. [consulta: 06 febrero 2022]
[250] Recurso en línea: *Privacy and security considerations for virtual health care visits. Guidelines for the health sector, February 2021.* Disponible en: https://bit.ly/3BZLNZX. [consulta: 06 febrero 2022]
[251] Op. Cit. p. 2.
[252] Op. Cit. p. 4-5.
[253] Recurso en línea: *Avoiding Abandoned Health Records: Guidance for Health Information Custodians Changing Practice*, *February 2019*. Disponible en: https://bit.ly/3bUw7wA. [consulta: 06 febrero 2022]
[254] Op. Cit. p. 1.
[255] Op. Cit. p. 3.

almacenadas las fichas o explicando cómo se podrán ejercer los derechos de acceso o portabilidad.[256]

En términos sancionatorios, la OPC ha sido objeto de críticas por carecer de esta clase de potestades a diferencia de las autoridades europeas; solo puede investigar denuncias, obligar auditorías, perseguir responsabilidad ante tribunales por infracciones a la *Privacy Act* o PIPEDA, publicar recomendaciones para el tratamiento de datos personales en el sector público y privado, realizar estudios relacionados a privacidad y promover la importancia de la materia.[257] Por esta razón, el gobierno federal patrocinó en 2020 una iniciativa (*Bill C-11 Digital Charter Implementation Act*) para adoptar la *Consumer Privacy Protection Act* —en reemplazo de PIPEDA— y crear tribunales con competencia exclusiva para conocer de las impugnaciones a las sanciones que podría determinar la OPC en términos similares al GDPR, es decir, multas millonarias calculadas en base a un cierto porcentaje de los ingresos brutos anuales de una compañía.[258] [259]

Por su parte, la IPC en virtud de PHIPA permite que, por ejemplo, ante el tratamiento de datos de salud en contravención a esta ley se sancione con multa de hasta CAD$200.000 y hasta un año de prisión si se trata una persona natural, o multa de hasta CAD$1 millón en el caso de las personas jurídicas (artículo 72.1 y 72.1 PHIPA), sin perjuicio de la pena que pudiere corresponderle al funcionario que personalmente cometió el ilícito o contaba con la autoridad suficiente para evitarlo (art. 72.3 PHIPA).

C. ESPAÑA.

Este país se rige por el GDPR (aprobado en 2016 y en plena vigencia desde 2018) y por la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD), cuyo objetivo es adaptar al ordenamiento jurídico español las disposiciones del primero y garantizar los derechos digitales de la ciudadanía de conformidad al artículo 18.4 de la Constitución española.

---

[256] Op Cit. p. 4.
[257] Recurso en línea: *About the OPC — What we do.* Disponible en: https://bit.ly/3GZI8iF. [consulta: 06 febrero 2022]
[258] Recurso en línea: *Privacy trends to watch in 2021: Canada modernizes its private-sector privacy laws, February 19, 2021, JDSUPRA.* Disponible en: https://bit.ly/3qgmmBa. [consulta: 06 febrero 2022]
[259] Recurso en línea: *Digital Charter Implementation Act, 2020*. Disponible en: https://bit.ly/3mXldfL. [consulta: 06 febrero 2022]

En particular, los datos de salud se definen en el GDPR como “datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud”.[260] Se trata de una categoría especial de datos personales que no está autorizada sin el consentimiento del titular, salvo en situaciones excepcionales como, por ejemplo, la existencia de razones de interés en el ámbito de la salud pública.[261] Esto sin perjuicio de lo que la judicatura determine como constitutivo de los datos de salud, tal como ocurrió con los datos de dopaje de un deportista, aunque no son considerados como tales por la AEPD, la Audiencia Nacional sí incluyó.[262]

La LOPDGDD replica el sentido de las disposiciones precitadas, agregando como obligatoria la designación de un delegado de PDP respecto de los centros sanitarios que estén legalmente obligados al mantenimiento de historias clínicas de los pacientes.[263] En términos simples, esta figura —regulada en el artículo 37 y siguientes del GDPR— consiste en una persona especialmente facultada para informar y asesorar al responsable del tratamiento de datos personales, supervisar a nivel interno el cumplimiento de las normas sobre PDP, cooperar y actuar como punto de contacto con la autoridad de control, entre otros.

Asimismo, debemos considerar lo que dispone la ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; en cuanto en el capítulo V se regula la historia clínica y los alcances de su uso, conservación y derechos de los pacientes, sin perjuicio de que todo lo relativo al tratamiento de datos personales se complemente por el GDPR y la LOPDGDD. En relación con los usos, esta ley obliga a que cada centro y servicio sanitario, establezca los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente, junto con determinar que el personal de administración solo pueda acceder a datos relacionados con sus propias funciones.

A nivel nacional, el organismo principal en la materia corresponde a la Autoridad Española de Protección de Datos (AEPD), sin perjuicio de que a nivel comunitario resulta fundamental

[260] Artículo 4.15 GDPR.
[261] Artículo 9 GDPR.
[262] Recurso en línea: La Audiencia Nacional fija que los datos de dopaje son datos de salud del deportista, IUSTEL. Disponible en: https://bit.ly/3EYuZoc. [consulta: 06 febrero 2022]
[263] Artículo 34 letra l) LOPDGDD.

el Comité Europeo de PDP —que se conforma por el director de una autoridad de control de cada Estado miembro de conformidad al art. 68 GDPR— y el Supervisor Europeo de PDP. Asimismo, existen autoridades de control a nivel autonómico como, por ejemplo, la Autoridad Catalana PDP o la Agencia Vasca de PDP.

Resultan relevantes dos guías de buenas prácticas de la AEPD; la primera está hecha para los pacientes y usuarios de la sanidad —lo más cercano que se puede encontrar sobre datos de salud—. En esta línea, el documento precisa que el tratamiento de datos en la sanidad debe respetar los principios de licitud, lealtad, transparencia, finalidad, minimización, exactitud, limitación en el plazo de conservación y calidad.[264]

El carácter informativo de la guía resalta los derechos ARCOP de los titulares, así como sugiere —para revocar el consentimiento— presentar una reclamación ante la autoridad de control o solicitar información, ser oído o impugnar decisiones automatizadas.[265]

En relación con los derechos de los titulares, es menester resaltar la vinculación entre el derecho a la portabilidad y la interoperabilidad que el GDPR incluye entre sus fundamentos:

> "Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que le conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e **interoperable**, y los transmitan a otro responsable del tratamiento. **Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos**. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato […] (el destacado es nuestro)".[266]

Una de las formas en que el GDPR y la LOPDGDD logra materializar sus disposiciones es por la vía de promoción de la cultura de PDP que tiene lugar entre la autoridad de control, los responsables y delegados de protección PDP y los titulares. Sin embargo, el

[264] Recurso en línea: Guía AEPD para pacientes y usuarios de la Sanidad, noviembre 2019. p. 8-9. Disponible en: https://bit.ly/3bV6Dip. [consulta: 06 febrero 2022]
[265] Op. Cit. p. 6-8.
[266] Considerando Nº 68 del GDPR.

complemento más eficaz es la fiscalización y posterior sanción cuyas penalidades resultan sustantivamente onerosas.

El artículo 83 GDPR establece las reglas de determinación de sanciones y las aplicables en casos de infracción. La AEPD debe ponderar la naturaleza, gravedad y duración de esta, así como la intencionalidad, medidas de mitigación que el responsable haya adoptado, reincidencia, entre otros factores.

En cuanto a la cuantía de la sanción, al tratarse de la vulneración a los principios básicos para el tratamiento, derechos de los interesados o transferencia transfronteriza de datos personales —operaciones que podrían involucrar datos de salud—, la AEPD puede cursar una multa administrativa de hasta €20 millones que, tratándose de una empresa, puede ser de hasta un 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor valor. Esto tuvo lugar a escala comunitaria cuando la autoridad de control de Luxemburgo sancionó con €746 millones por graves infracciones al GDPR, constituyendo la multa más alta de la que se tenga registro.[267] Sin embargo, aún no es factible conocer los detalles de la infracción debido a que la autoridad de control está obligada a respetar normas secreto profesional.[268]

En relación con la jurisprudencia de la AEPD relativa a datos de salud, se ha multado con €40.000 a un hospital privado gallego que incluyó la historia clínica de una paciente al sistema compartido con el Servicio Gallego de Salud, pese a que acudía a consultas privadas.[269] Asimismo, se sancionó con €5.000 a un médico por extraviar las imágenes grabadas durante una intervención quirúrgica a una paciente en 2014, impidiéndole contrastar la opinión con otros facultativos.[270] Además, se multó con €50.000 a un centro de salud que cedió a entidades financieras los datos personales de un titular que cotizó una operación de reducción estomacal, sin llegar a suscribir el contrato.[271]

---

[267] Recurso en línea: *CNPD vs. Amazon, ¿the largest GDPR fine on record – what do we know so far?, August 16, 2021, JDSUPRA.* Disponible en: https://bit.ly/3kDMe6z. [consulta: 06 febrero 2022]
[268] Recurso en línea: *Decision regarding Amazon Europe Core S.Á R.L.*, *August 6, 2021, CNPD*. Disponible en: https://bit.ly/31ChhZv. [consulta: 06 febrero 2022]
[269] Recurso en línea: Multa a un hospital por compartir datos procedentes de aseguradoras privadas con el servicio de salud gallego, 18 enero, 2019. Disponible en: https://bit.ly/3mVQxLI. [consulta: 06 febrero 2022]
[270] Recurso en línea: Multa de 5.000 euros a un médico por perder la grabación de una operación, 13 noviembre 2018. Disponible en: https://bit.ly/3CZCaMf. [consulta: 06 febrero 2022]
[271] Procedimiento AEPD Nº PS/00206/2020.

Recientemente la AEPD ha abierto una investigación contra la Comunidad de Madrid por una brecha de seguridad en el sitio web para obtener el certificado COVID que dejó al descubierto los datos personales de miles de ciudadanos, incluyendo a integrantes de la monarquía y del gobierno.[272]

Por último, es importante considerar la Carta de Derechos Digitales que, en julio de 2021, el Gobierno Español publicó. Esta pese a no tener carácter normativo, sí "ofrece un marco de referencia para garantizar los derechos de la ciudadanía en la nueva realidad digital" recogiendo una serie de principios y derechos orientativos de futuras legislaciones.[273] Este documento regula, específicamente en su Título XXIII, el "Derecho a la protección de la salud en el entorno digital" y destaca especialmente el numeral 3º en cuanto exhorta al sistema de salud a promover el desarrollo de sistemas de información que aseguren la interoperabilidad, el acceso y la portabilidad de la información del paciente.[274]

[272] Recurso en línea: Protección de Datos abre una investigación sobre la brecha de seguridad de Madrid que destapó datos del rey. Disponible en: https://bit.ly/3odf8uT. [consulta: 06 febrero 2022]

[273] Recurso en línea: El Gobierno de España adopta la Carta de Derechos Digitales, 15 julio 2021. Disponible en: https://bit.ly/3bRPI06. [consulta: 06 febrero 2022]

[274] XXIII

Derecho a la protección de la salud en el entorno digital

1. Con arreglo a las normas de todo rango que resulten aplicables, todas las personas tendrán acceso a los servicios digitales de salud en condiciones de igualdad, accesibilidad y universalidad, así como a la libre elección de la asistencia presencial. Se adoptarán medidas para garantizar este acceso y evitar la exclusión de colectivos en riesgo.
2. Los poderes públicos promoverán que la investigación y la tecnología contribuyan al logro de una medicina preventiva, predictiva, personalizada, participativa y poblacional.
3. El sistema de salud promoverá el desarrollo de sistemas de información que aseguren la interoperabilidad, el acceso y la portabilidad de la información del paciente.
4. El empleo de sistemas digitales de asistencia al diagnóstico, y en particular de procesos basados en inteligencia artificial no limitarán el derecho al libre criterio clínico del personal sanitario.
5. Los entornos digitales de salud garantizarán, conforme a la legislación sectorial, la autonomía del paciente, la seguridad de la información, la transparencia sobre el uso de algoritmos, la accesibilidad y el pleno respeto de los derechos fundamentales del paciente y, en particular, su derecho a ser informado o renunciar a la información y a consentir en el tratamiento de sus datos personales con fines de investigación y en la cesión a terceros de tales datos cuando tal consentimiento sea requerido.
6. Los poderes públicos impulsarán el acceso universal de la población a sistemas de telemedicina y teleasistencia, así como a los dispositivos tecnológicos desarrollados con fines terapéuticos o asistenciales en condiciones adecuadas de conectividad. Se procurará establecer que el acceso a estos dispositivos cuando se facilite a título gratuito por un fabricante o proveedor no pueda condicionarse a la cesión a aquellos de los datos personales del paciente.

D. URUGUAY.

La PDP corresponde a un derecho humano en conformidad al artículo 72 del texto constitucional uruguayo, que dispone que la enumeración de derechos, deberes y garantías allí consagrada no es de carácter taxativo.

La ley de datos protección de personales, en tanto, es la Nº 18.331 de 2008, que considera los DPS como datos sensibles y especialmente protegidos, siendo su régimen jurídico más estricto en comparación a otra clase de datos personales. De ahí que no se puedan comunicar sin previo consentimiento de los titulares, salvo que sea necesaria su divulgación por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, en cuyo caso es obligatorio preservar la identidad de los titulares de los datos mediante mecanismos de disociación adecuados cuando ello sea pertinente (artículo 17).

A diferencia de Chile, la ley uruguaya se refiere específicamente a los datos de salud en el artículo 19, que prevé que "los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley".

El precitado cuerpo legal, en su capítulo VII, establece a la Unidad Reguladora y de Control de Datos Personales (URCDP) como el órgano de control desconcentrado dentro de la AGESIC, encargado de realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la ley, en conformidad al artículo 34. Estos estándares son compatibles con las exigencias del GDPR por la decisión de adecuación de la CE emitida el año 2012, que reconoció a Uruguay como el segundo país de Sudamérica, después de Argentina, en estar habilitado para el tráfico transfronterizo de datos personales.[275]

La URCDP cuenta con amplias atribuciones para solicitar información de los regulados, así como intervenir e incluso incautar documentos y archivos cuando sea imprescindible. Sus potestades sancionatorias están sujetas a reglas de graduación en atención a la gravedad,

[275] Decisión 2012/484/UE de Ejecución de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales.

reiteración o reincidencia en la infracción y de conformidad al artículo 35, estas pueden consistir en una observación, apercibimiento, multa de hasta 500.000 unidades indexadas, suspensión de la base de datos respectiva por hasta cinco días o bien la clausura de esta.

La robustez de estas sanciones, a su vez viene acompañada de la prohibición de suspender la aplicación de estas medidas en caso de que la persona o entidad sancionada las impugne. Por otra parte, la URCDP al igual que el resto de las autoridades de control a nivel comparado, emite guías de buenas prácticas que se han referido a los datos de salud.

La más reciente se publicó en 2018 y, junto con precisar la normativa aplicable, recomienda a los centros de salud contar con "una política y un documento que describa los procedimientos relativos a la seguridad de información, así como un responsable de seguridad que desarrolle programas de difusión y sensibilización del personal sobre las medidas dispuestas en las políticas de seguridad".[276] Asimismo, aconseja adoptar medidas necesarias para mantener la integridad en caso de traslado de información o documentos, y si se destruyen, este procedimiento no debe permitir la recuperación posterior.[277] Todo esto resulta igualmente aplicable respecto de tratamientos de datos realizados por terceros a cuenta del centro asistencial.[278]

Adicionalmente, emitió recomendaciones durante la emergencia sanitaria provocada por el COVID-19, recalcando el respeto al principio de minimización, junto con la capacitación constante del personal asistencial acerca del cuidado de la información personal y las consecuencias penales asociadas a la revelación de dicha información.[279] Estas guías encuentran su complemento en aquellas que publica la AGESIC, por ejemplo para la disociación y anonimización de datos personales en el ámbito de salud, en que enfatiza que la autoridad provee de un procedimiento para llevar a cabo esta operación, incluyendo un proceso de pre-anonimización, así como la entrega de alternativas para llevarlo a cabo.[280]

---

[276] Recurso en línea: Protección datos de salud URCDP, 2018. p. 3. Disponible en: https://bit.ly/3CXsba1. [consulta: 06 febrero 2022]
[277] Op. Cit.
[278] Op. Cit.
[279] Recurso en línea: Recomendaciones URCDP para el tratamiento de datos personales ante la situación de emergencia sanitaria nacional, 2020. Disponible en: https://bit.ly/3jxz3DA. [consulta: 06 febrero 2022]
[280] Recurso en línea: Guía AGESIC de disociación y anonimización de datos personales en el ámbito de la salud, 2019. Disponible en: https://bit.ly/3B8RaWc. [consulta: 06 febrero 2022]

Entre la jurisprudencia de la URCDP destaca el dictamen Nº12/018 que remarca cuatro elementos de relativos al tratamiento de los datos de salud.[281] El primero consiste en la propiedad del paciente acerca de su historia clínica sin perjuicio de que su registro se encuentre bajo la custodia del prestador de salud, siguiendo un criterio económico más que propio de la autodeterminación informativa. En segundo lugar, el sistema y la plataforma de Historia Clínica Electrónica Nacional son de carácter obligatorio para los prestadores incorporados al Sistema Nacional Integrado de Salud, quienes quedan legalmente autorizados a registrar la información necesaria para el funcionamiento de la plataforma, debiendo respetar la ley Nº 18.331 sobre PDP. Tercero, que el acceso a la información clínica por parte del personal médico y administrativo mediante la Plataforma de Historia Clínica Electrónica Nacional implica una comunicación de datos personales que requiere del consentimiento previo expreso y escrito del titular, salvo en ciertas circunstancias taxativas. Cuarto, que el tratamiento de los datos de salud debe cumplir con todos los principios en materia de PDP, así como con el secreto profesional.

Por otra parte, ante una consulta presentada por el Servicio de prevención y Salud en el Trabajo respecto de la historia clínica laboral, el Consejo Ejecutivo de la URCDP ha resuelto, a través del dictamen Nº 12/021, que esta sí se ajusta a la legislación vigente.[282] En consecuencia, es factible que los empleadores mantengan una ficha clínica de carácter laboral exclusivamente para el control de enfermedades que puedan afectar la relación laboral, la que debe circunscribirse al principio de minimización, es decir, los datos deben ser los imprescindibles para el cometido fijado. Una vez finalizada la relación laboral, los datos deben ser eliminados salvo aquellos que deban ser conservados para cumplir obligaciones legales, que deberá estar bloqueada. Por último, recomienda la imposición de niveles diferenciados de acceso, medidas de seguridad proporcionales, así como otras medidas de responsabilidad proactiva, la realización de una evaluación de impacto y la designación de un delegado de PDP.

Otro dictamen relevante es el Nº 11/021 dictado a raíz de una consulta realizada acerca de los datos que figuran en los recibos que se entregan en una red de cobranzas al abonar gastos mutuales. Aquí el Consejo Ejecutivo resolvió que “instituciones médicas que envíen a las redes de cobranzas información de sus usuarios para el pago de medicación o de estudios médicos, deberán hacerlo en forma tal que los datos que surjan en las impresiones

[281] Dictamen URCDP Nº 12/018.
[282] Dictamen URCDP Nº 12/021.

de los tickets emitidos sean proporcionales, indicando los rubros abonados, sin especificar, por ejemplo, médico tratante, especialidad, entre otros.".[283] Estas instituciones tienen la obligación de informar a todos sus usuarios cada vez que realicen cambios en los procedimientos internos que afecten sus datos personales, debiendo requerir el consentimiento cada vez que sea necesario, en consonancia con el principio de finalidad.

3.- SÍNTESIS DE LOS CAPÍTULOS I, II Y III.

Tomando en cuenta los nudos críticos detectados luego de desarrollar y analizar el marco jurídico de las fichas clínicas y de la interoperabilidad en los Capítulos I y II —respectivamente—, podemos observar que la PDP constituye un punto insoslayable para la adecuada implementación de la FCEI.

En resumidas cuentas, cada ficha clínica constituye información de carácter sensible, lo cual obliga a que cualquier política pública que las involucre deba adoptar resguardos proporcionales a la naturaleza de esos DP.

Corolario de lo anterior es que la pronta publicación del PDLPDP constituya una condición *sine qua non* previo a que la autoridad avance en la FCEI, puesto que antes que todo debe estar garantizar el pleno respeto a los derechos de los pacientes.

Sin embargo, no podemos aseverar que los pacientes en la actualidad tengan garantizadas las condiciones jurídicas y materiales suficientes para estar en pleno control de sus DPS como lo exige el artículo 19 Nº 4 del texto constitucional o el artículo 8º de la Carta Europea de DD.FF., ello se desprende de las brechas entre la LPVP y el GDPR a que antes nos hemos referido. Al respecto debemos recordar que el CDH exhorta a los Estados para que "apliquen salvaguardias administrativas, técnicas y físicas para garantizar que los datos se procesen de manera lícita y que este procesamiento resulte necesario en función de sus fines, y garanticen la legitimidad de esos fines y la precisión, integridad y confidencialidad del procesamiento".[284]

El análisis de la experiencia internacional de Australia, Canadá, España y Uruguay permite construir ejemplos elocuentes para graficar la dilación legislativa de Chile en materia de

[283] Dictamen URCDP Nº 11/021.
[284] CDH. El derecho a la privacidad en la era digital. Resolución aprobada por el Consejo de Derechos Humanos ONU el 7 de Octubre de 2021, Nº 48/4. p. 6.

FCEI y, a su vez, permiten resaltar la preocupante situación de indefensión en que se encuentran los pacientes en la actualidad.

Para graficar la importancia del control de las personas sobre sus DP basta recordar que el TJUE las dos veces que invalidó los convenios transfronterizos entre la UE y EE.UU. invocó como fundamento principal la falta de garantías que este último país contemplaba para los ciudadanos europeos.[285] [286]

Lo anterior permite comprender por qué a nivel comparado los textos constitucionales de Argentina (artículo 43), Brasil (art. 5º literal LXXII), Bolivia (arts. 130 y 132), Colombia (art. 15), Ecuador (arts. 66 literal 19 y 92), Perú (arts. 2º literal 6º y 200 literal 3º) y México (arts. 6º, 16, 20, y 28) consagren disposiciones a los derechos ARCO y al habeas data, una materia que por cierto será abordada en el proceso constituyente chileno.

[285] STJUE Rol Nº C-362-14, considerando 91: "[...] de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de estos.

[286] STJUE Rol Nº C-311-18, considerando 176: "[...] de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personales contra los riesgos de abuso".

CONCLUSIONES Y RECOMENDACIONES DE POLÍTICA PÚBLICA.

1.- PDL PARA ESTABLECER EXPRESAMENTE QUE LOS DATOS DE SALUD DE LAS PERSONAS DEBEN INTEROPERAR.

A la luz de los resultados de nuestra investigación quedan claras las razones que justifican que se discuta una norma legal que modifique la ley de derechos y deberes de los pacientes, estableciendo la interoperabilidad de la ficha clínica y todos y cada uno de los documentos que la componen.

Esta obligación debiera ser aplicable a todo prestador, tanto público como privado, individual o institucional.

Adicionalmente, sería aconsejable que la iniciativa incluya conceptos propios de la ciencia o arte para evitar confusiones o dificultades en la aplicación de la ley, entre los cuales podrían estar la interoperabilidad y los principios que la OMS promueve en este ámbito. Esto sin perjuicio de dejar a la potestad reglamentaria los aspectos más de detalle.

Asimismo, idealmente debe incorporarse un deber respecto de un organismo público determinado de modo que sea la entidad competente para definir y actualizar los estándares necesarios (por ejemplo, HL7 FHIR) por la vía reglamentaria. A estos efectos debe tenerse en cuenta que conforme al DFL N° 1 de 2006, corresponde al Ministerio de Salud dictar normas técnicas y definir estándares para el sector salud en su conjunto.

Así las cosas, se podría constituir un sistema interconectado de las fichas clínicas, lo cual es fundamental para un acceso y uso oportuno por los distintos prestadores ajustado a principios como la proporcionalidad, minimización y calidad con pleno respeto de los titulares.

A su vez, se estaría propiciando una concreción más eficiente y eficaz del deber estatal en materia de salud en el marco de las a las directrices del principio de coordinación emanadas de la Corte Suprema.

Esto último se traduciría en que los distintos organismos públicos que participan del área de salud puedan contar con un sistema unificado que les facilite el ejercicio de sus facultades, optimizando el impacto económico tanto para las personas, así como del fisco, todo lo cual fue desarrollado en el párrafo sobre los beneficios de las FCEI.

2.- POLÍTICA NACIONAL DE INTEROPERABILIDAD.

Aconsejamos que la implementación de la interoperabilidad no se circunscriba únicamente al sector salud, siendo deseable que el Estado desarrolle una Política Nacional de Interoperabilidad, así como lo ha realizado previamente en otros ámbitos como son la seguridad pública, la ciberseguridad o la inteligencia artificial, por nombrar sólo algunos.

Ello por cuanto, en el capítulo III referente a la interoperabilidad quedan de manifiesto las razones que hacen recomendable extender su desarrollo al grueso de la actividad estatal para lo cual resulta aconsejable replicar la experiencia del EIF.

Claramente constituye un avance el reglamento de la ley de transformación digital, pero no es suficiente en cuanto los instrumentos infra legales no son capaces de dotar la estabilidad requerida para el impulso de una política pública esenciales para la transformación digital del Estado bajo criterios de optimización respetuosos de los derechos de las personas.

3.- MEDICIÓN DE LOS ÍNDICES DE MADUREZ DE LA INTEROPERABILIDAD TANTO EN EL SECTOR SALUD, ASÍ COMO EN EL RESTO DE LA ADMINISTRACIÓN DEL ESTADO.

Relacionado a lo anterior, hemos observado que ámbito de la interoperabilidad excede con creces al área de salud, siendo el mejor ejemplo de aquello el EIF. Tratándose de la gobernanza de los datos, es relevante que la autoridad disponga de información casi en tiempo real respecto de los niveles de madurez de interoperabilidad existentes tanto en el sector público como privado, tal como recomienda David Rowlands para el caso australiano.

Siguiendo a la OCDE, nos referimos a "una herramienta que mid[a] el estado de un proceso o conjunto de procesos 'tal como está', y que describ[a] aquellos componentes críticos del mismo que conducen a obtener mejores resultados".[287] Puntualmente, se trata de determinar el "grado en el cual una organización —o unidad organizacional— desarrolla, asimila e implementa buenas prácticas de interoperabilidad.[288]

En este sentido, es importante que la medición considere los cuatro niveles generales de interoperabilidad (intra-administrativo, horizontal, vertical y regional o transfronterizo) como asimismo aquellos niveles específicos del sector salud (técnica, sintáctica, semántica y organizacional).

[287] BID. El ABC de la interoperabilidad de los servicios sociales: Guía para los Gobiernos, 2019. p. 6.
[288] Op. Cit., p. 14.

Acto seguido, basándonos en el caso uruguayo, estimamos que es necesario calificar cada uno de los diferentes niveles de interoperabilidad con respuestas predeterminadas que van de uno a cinco:

> 1.- "Inicial: El trámite o servicio está en línea y cumple con criterios de seguridad y protección de datos personales.
> 2.- Mejorado: El trámite o servicio está publicado de acuerdo a los lineamientos de Modelo de Atención a la Ciudadanía. Además, cumple con requisitos de usabilidad y admite pago en línea en caso de que corresponda.
> 3.- Gestionado: El trámite o servicio incorpora la interoperabilidad entre organismos y permite realizar seguimiento sobre su estado.4.- Completo: Se realizan acciones de monitoreo para medir el nivel de satisfacción de las personas que utilizan el trámite o servicio. Además, adopta mejores prácticas para la documentación interna, facilitando su evolución y el trabajo de quienes colaboran en el organismo.
> 5.- Óptimo: Define y usa indicadores para tomar acciones de mejora con base en los datos que se registran en las acciones de monitoreo del nivel anterior. Además, integra firma digital, eliminando pasos presenciales y controles manuales.".[289]

Finalmente, una vez que cada aspecto está evaluado podemos extraer promedios generales o bien específicos de un determinado nivel de interoperabilidad. Por ejemplo, la interoperabilidad horizontal en el nivel semántico.

A través de la cuantificación de los grados de interoperabilidad, la autoridad dispondrá de información de calidad que le permitirán focalizar esfuerzos y recursos en las áreas más inmaduras.

4.- UNIFORMIDAD Y ACTUALIZACIÓN DE ESTÁNDARES.

La certeza jurídica es vital para que todos los actores del sector salud estén informados sobre los estándares vigentes. En esta línea, el obstáculo que hemos observado es que el modelo de gobernanza de la normalización de estándares no resulta fácil de dilucidar considerando que están entrecruzados el INN y el CENS con la facultad de la SEGPRES para la adopción de normas técnicas en cuanto posee competencia sobre el Gobierno Digital.

[289] Recurso en línea: AGESIC — Modelo de madurez de calidad de trámites y servicios digitales de fecha 04/06/2021. Disponible en: https://bit.ly/3ygZhAh. [consulta: 06 febrero 2022]

Frente a este escenario, estimamos recomendable modificar urgentemente la gobernanza de estándares aplicables a la interoperabilidad del sector salud existiendo para dicha tarea dos alternativas.

La primera sería una autoridad con competencia para definir los estándares de interoperabilidad sin circunscribirlo necesariamente al área de la salud, quedando, en consecuencia, todos centralizados. Lo anterior corresponde al caso uruguayo, cuyo Instituto de Normas Técnicas aborda los estándares para la salud, así como para todo el ámbito público.

Una segunda alternativa sería la adopción de una autoridad con competencia exclusiva para determinar los estándares y normas técnicas aplicables para la interoperabilidad en el sector salud. Por ejemplo, este modelo sería el adoptado por Canadá y también el que buscaría implementar próximamente Australia.

Sea cual sea la opción, lo importante es trabajar para revertir la des gobernanza de estándares de interoperabilidad en salud que se advierte en Chile, imitando las experiencias exitosas de otros países al implementar las normas técnicas de más frecuente aplicación.

A contrario sensu, desaconsejamos impulsar políticas públicas de interoperabilidad en el sector salud mientras no sea esclarecida la gobernanza de estándares. Asimismo, el escenario ideal sería la implementación de la salud digital en un contexto donde las reformas en PDP y ciberseguridad estén en plena vigencia, aunque sabemos que ello depende de factores exógenos ajenos a este estudio.

Por ello, no podemos dejar de advertir los riesgos derivados de reformas institucionalmente inorgánicas en materias digitales. Es difícil asimilar que la APDP se relacione a través del presidente de la República a través del MINECON, mientras que emisión de las NT de interoperabilidad sean de competencia de la SEGPRES y la regulación de los datos financieros corresponda a la CMF —según PDL FINTECH—, es decir, una entidad que se relaciona con el presidente de la República a través del Ministerio de Hacienda.

Paradojalmente, el PDLPDP pretende modificar la concepción economicista de la LPVP, pero al mismo tiempo busca entregarle su supervisión a dicho Ministerio. Siguiendo esta línea, el grueso de la labor de la SEGPRES consiste en la tramitación legislativa de todos los proyectos de ley que sean de interés del Ejecutivo de turno, por lo cual su *know how* se aparta radicalmente de aquel requerido para el desarrollo digital y de la FCEI.

5.- SISTEMATIZACIÓN DE LOS DATOS PERSONALES DE SALUD Y EVALUACIÓN DE IMPACTO PREVIO.

Al abordar las fichas clínicas la PDP resulta un tópico ineludible donde Chile no destaca particularmente por estar en la vanguardia. La razón de ello se debe a que la LPVP sea de fines de la década del noventa, es decir, anterior a la masificación de internet y a la reforma constitucional que consagró la autodeterminación informativa.

Adicionalmente, la LPVP fue concebida para preocuparse del establecimiento de ciertos mínimos en que debe operar el mercado de los datos personales antes que privilegiar el control que los titulares de los datos personales poseen respecto de su información personal.

Corolario de ello es la preeminencia que el legislador le otorgó al tratamiento por parte de organismos públicos en desmedro de los privados, careciendo ambos en cualquier caso de la supervisión de una autoridad independiente con atribuciones suficientes como para imponer gravosas sanciones de carácter administrativo, que incentivaran el cumplimiento normativo.

En suma, la LPVP no hace más que contradecir la mayor parte de las reglas, principios y valores existentes a nivel comparado, cuyo paradigma lo conforman el GDPR junto a la Carta Europea de DD.FF. Esta situación debiera revertirse con la aprobación del proyecto de ley que se tramita en el Congreso Nacional, considerando de que la PDP es un derecho que es un medio irremplazable para el ejercicio de otros derechos fundamentales reconocidos a la persona.

Además, en voz del artículo 19 Nº 4 CPR, el PDLPDP establecería las formas y condiciones para el tratamiento de datos personales efectuado por personas naturales y jurídicas pertenecientes al sector público o privado, logrando finalizar la transición hacia un marco regulatorio cuya piedra angular sea la capacidad de control de las personas sobre sus propios datos personales. De paso concluiría la transición y perfeccionamiento del sistema de fuentes con relación a la garantía fundamental de autodeterminación informativa que excluye su desarrollo por vías infralegales, a diferencia de lo que ocurre en el presente.

Lo anterior tendría directo impacto en el tratamiento de datos personales que tiene lugar en el sector salud, uno donde hasta hace no tanto tiempo no era tan claro que los pacientes fueran los titulares de sus fichas clínicas producto de que los prestadores de salud en

cuanto administradores de estos instrumentos declaraban por sí y ante sí su propiedad. En este sentido, bajo el nuevo marco jurídico los prestadores tendrán los incentivos para implementar modelos de cumplimientos y estar certificados ante el organismo de control.

El cambio de posición del paciente hacia el centro del proceso asistencial tiene por efecto facilitar el ejercicio de los derechos ARCOP, aumentar los deberes para los responsables, delegados y mandatarios en el tratamiento de datos personales y, en definitiva, elevar estándares globales aplicables a esta materia. El incentivo para que lo anterior se produzca pasa por la amenaza latente de un vigoroso régimen sancionador que es el principal aliciente para que se verifique el cambio cultural en favor de la PDP.

Asimismo, los titulares estarían interesados debido a que con la ley vigente propicia su indefensión, quedando expuestos ante, por ejemplo, una transacción comercial de sus DPS. Más aún, se incrementan estos riesgos tratándose de datos de salud de NNA.

Tanto es así, que incluso sería aconsejable despachar las normas relativas al ámbito de la salud en el caso de que se mantenga la dilatación del proyecto marco.

Ahora bien, sin perjuicio de las bondades del PDLPDP, consideramos que es perfectible en cuanto prescinde de regular regulación el deber de impacto y consulta previa consagrados por los artículos 35 y 36 del GDPR, respectivamente. Imaginemos una operación de concentración entre actores dominantes del área salud.

La primera disposición obliga a realizar una evaluación de impacto cuando “sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas […]”, siendo de carácter obligatorio en caso de tratamientos que impliquen el uso de datos de salud, impliquen toma de decisiones automatizadas, perfil de sujetos, sean a gran escala, para atender finalidades distintas, entre otros.

Mientras tanto, el deber de consulta previa es aquel que procede cuando una evaluación de impacto del artículo 35 muestra que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

En efecto, la asimilación de ambas normas dentro del derecho interno nacional sería favorable de modo que la implementación de políticas de interoperabilidad ocurra con pleno respeto a los derechos de los titulares. De igual modo, sería conveniente adoptarla en casos

en que la autoridad pretenda aplicar inteligencia artificial para la distribución de pacientes en el sistema de salud o bien, tal como ocurrió con la aplicación denominada *CoronApp.*

Por último, consideramos que junto a la publicación del PDLPDP es urgente la pronta suscripción y ratificación del Convenio 108 y sus protocolos por parte del presidente de la República. En este sentido, las TIC producto de su constante evolución —sobretodo las del área de la salud— van añadiendo nuevos desafíos a la privacidad, que van sumándose a los ya existentes y frente a este contexto el apoyo coordinado y decidido de la comunidad internacional emerge como una herramienta irremplazable, lo cual no es óbice a los esfuerzos multilaterales que puedan desarrollarse eventualmente en América Latina y el Caribe en este ámbito. Lo anterior sin perjuicio de que aún falta bastante para pensar en regulaciones eficaces para el establecimiento de FCEI capaces de sobreponerse a los límites fronterizos de, al menos, Sudamérica.

6.- AGENCIA DE PROTECCIÓN DE DATOS PERSONALES Y DE CIBERSEGURIDAD.

Corresponde poner de manifiesto los problemas derivados de diluir entre diversas entidades públicas las eventuales competencias de una Agencia de Protección de Datos Personales, en cuanto organismo de control para velar por el respeto de las normas sobre PDP.

El caso más notorio consiste en el artículo 15 bis del PDL Pro-consumidor donde el legislador en una primera instancia pretendió dotar al SERNAC de competencia amplia para velar por infracciones a la LPVP hasta que culmine su tramitación el proyecto marco, cuestión que sólo fue enmendado durante la Comisión Mixta y finalmente restringido a afectaciones en los datos de carácter económico del título III LPVP.

Otro intento del legislador fue el PDL FINTECH que dota de amplias competencias a la CMF para determinar las condiciones del tratamiento de datos personales del cliente financiero en el mercado de un Sistema de Finanzas Abiertas.

Estas circunstancias nos llevan a estimar que la pronta publicación de la ley marco de datos personales es imprescindible no tan sólo por la reivindicación del titular en el centro de los tratamientos sino también porque mientras se dilata otros organismos van capturando sus potenciales atribuciones, llámese SERNAC, CMF u otros.

Por lo anterior, es importante despejar el ámbito de las atribuciones de la futura agencia de datos personales porque de lo contrario la posibilidad de que vuelva a consagrarse una autoridad con poder de fiscalización simbólico y engorroso aumente.

Por otro lado, es relevante la pronta modernización de los delitos informáticos según el Convenio de Budapest y, junto a lo anterior, avanzar en una legislación marco de ciberseguridad. Ello por cuanto, por más que se publique el PDL de delitos informáticos, es fundamental avanzar hacia una institucionalidad que ofrezca mucho más que un mero catálogo de tipos penales. Las complejidades derivadas del espacio virtual justifican que exista un ecosistema jurídico-administrativo capaz de disminuir los espacios de impunidad. De ahí que sea importante que promesas tales como la que el presidente de la República hizo en su última cuenta pública sean cumplidas.[290]

Podemos sostener que los pacientes siempre gozarán de una posición de menor indefensión respecto de su información personal si cuentan con institucionalidades distintas y complementarias como la APDP y otra con competencia en materias de ciberseguridad.

7.- TRANSFORMACIÓN DIGITAL DEL SECTOR SALUD Y DIGITALIZACIÓN DE LAS FICHAS CLÍNICAS CON PLENO RESPETO A LA GARANTÍA FUNDAMENTAL DE AUTODETERMINACIÓN INFORMATIVA.

Somos conscientes de la estrechez del erario, pero también sabemos que sólo será posible gozar de los beneficios de las FCE cuando sean marginales aquellas cuyo único soporte sea el físico. Por ello es necesario tender hacia la continuidad de políticas públicas, especialmente cuando buscan profundizar la interoperabilidad de las fichas clínicas.

Es deseable no reiterar experiencias como la ocurrida con la CMI, la cual a pesar de que sus beneficiarios eran cerca de 13 millones de personas y constituía un esfuerzo elocuente por avanzar en la implementación de la interoperabilidad, la falta de continuidad gubernamental la condenó al fracaso. Algo bastante semejante ocurrió con la iniciativa Hospital Digital, aunque en ese caso la rotación fue interna a nivel ministerial.

Ahora bien, es fundamental remarcar que la decisión de impulsar la transformación digital en el sector salud, incluyendo la modernización la uniformidad de estándares aplicables,

[290] Recurso en línea: Presidente Piñera anuncia proyecto de ley que crea la Agencia Nacional de Ciberseguridad. Disponible en: https://bit.ly/3ygZzXT. [consulta: 06 febrero 2022]

FCE y FCEI, pasa por las autoridades ejecutivas. Son ellos quienes tienen por mandato ponderar la evidencia y el equilibrio fiscal con la política.

Junto con lo anterior, es importante que la materialización de estas políticas públicas tome en consideración las reglas y principios básicos sobre protección de DPS por cuanto una vulneración a este derecho podría tener también consecuencias en el derecho fundamental de protección de la salud. Por lo tanto, es relevante establecer mecanismos para garantizar el control de los pacientes respecto de su información personal a través del ejercicio de los derechos ARCOP. En ese contexto, la FCEI, al permitir la portabilidad a intercambio de información, contribuye a un más eficiente y eficaz ejercicio del libre e igualitario acceso a las acciones de promoción, protección, recuperación y rehabilitación del individuo por parte del Estado.

Por ello es beneficioso que las empresas europeas que operan en el territorio nacional estén adecuando sus tratamientos de datos personales al GDPR como consecuencia de su aplicación global, lo cual no obsta a que la reforma a la LPVP no sea todavía realidad.

Así las cosas, la interoperabilidad de las fichas clínicas debe ser impulsada desde una concepción cimentada en el control de la persona respecto de su información personal cuyo sustento es la garantía fundamental de autodeterminación informativa, la cual a su vez es condición para un correcto ejercicio del derecho de protección a la salud.

A este respecto será muy importante tener presente los cambios que la Convención Constitucional realice con relación al catálogo de derechos digitales, que hoy básicamente está limitado a lo está consagrado por el artículo 19 Nº 1 y Nº 4.

8.- NO PERMITIR QUE LAS BARRERAS IMPIDAN EL LOGRO DEL OBJETIVO FINAL.

Somos conscientes de que existen al menos siete barreras de distinta naturaleza que obstaculizan la implementación de la FCEI. La propuesta contenida en este estudio no corresponde a una política pública de rápida y fácil implementación, dadas las barreras legales, culturales y de política pública que es necesario superar para que la información circule.

En efecto, las normas legales que requerirían modificarse por la implementación de la FCEI son bastantes y constituye un hecho público y notorio que las leyes no avanzan al mismo ritmo que se les necesita. En tanto, el factor cultural es insoslayable teniendo presente todo

el personal médico y administrativo tanto de zonas urbanas como rurales estaría obligar a interiorizarse en una materia que para muchos de ellos será completamente nueva, como podrían ser los estándares aplicables a cada nivel o los principios de las FCEI. Algunos por cierto podrían ser reacios a los cambios y entrampar la idea.

De ahí que sea imprescindible que la autoridad encargada de desarrollar la FCEI mantenga la firme convicción en el proyecto pudiendo apoyarse en los beneficios que se derivan para toda la cadena del proceso asistencial: pacientes, personal médico y administrativo, organismos públicos sectoriales, aseguradoras y al Estado en un sentido amplio.

BIBLIOGRAFÍA.

❖ DOCTRINA

➢ NACIONAL

- ÁLVAREZ, Daniel. 2016. Acceso a la información pública y protección de datos personales: ¿Puede el consejo para la transparencia ser la autoridad de control en materia de protección de datos? [en línea] RDUCN, Vol. 23. Núm. 1 <https://bit.ly/3oQgkpT> [consulta: 06 febrero 2022]
- ÁLVAREZ, Daniel. 2020. La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa. [en línea] Revista Chilena de Derecho y Tecnología, Vol. 9. Núm. 1. <https://bit.ly/3oQgkpT> [consulta: 06 febrero 2022]
- BENUSSI, Carlo. 2020. Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes. [en línea] Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 1 <https://bit.ly/3m1bwfl> [consulta: 06 febrero 2022]
- BORDACHAR, Michelle. 2019. Los datos de salud en el proyecto de ley de protección de datos personales. [en línea] El Mercurio online. 4 octubre, 2019 <https://bit.ly/3kvQTFQ> [consulta: 06 febrero 2022]
- CERDA, Alberto. 2003. Autodeterminación informativa y leyes sobre protección de datos. [en línea] Revista Chilena de Derecho Informático, Núm. 3. <https://bit.ly/3yjSqWM> [consulta: 06 febrero 2022]
- CERDA, Alberto. 2003. Intimidad de los trabajadores y tratamiento de datos personales por los empleadores. [en línea] Revista Chilena de Derecho Informático, Núm. 2. <https://bit.ly/30nysOq> [consulta: 06 febrero 2022]
- CERDA, Alberto. 2012. Legislación sobre protección de las personas frente al tratamiento de datos personales. [en línea] Apuntes de clases, Centro de Estudios en Derecho Informático <https://bit.ly/3F4BvKB> [consulta: 06 febrero 2022]
- CONTRERAS, Pablo y TRIGO, Pablo. 2019. Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. [en línea] Revista Chilena de Derecho y Tecnología, Vol. 8, Núm. 1. <https://bit.ly/3yi9YCC> [consulta: 06 febrero 2022]

- CONTRERAS, Pablo. 2020. El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena. [en línea] Estudios constitucionales Vol. 18, Núm. 2, Santiago <https://bit.ly/3IJxhdf> [consulta: 06 febrero 2022]
- CUMPLIDO, Francisco. 1997. Análisis del anteproyecto de ley sobre protección de datos personales elaborado por el Ministerio de Justicia (1990-1994). [en línea] Ius et Praxis Vol. 3, Núm. 1 <https://bit.ly/3GGWVhd> [consulta: 06 febrero 2022]
- DELOITTE. 2021. La evolución de la ciberseguridad en el sector de la salud. [en línea] Santiago, Chile <https://bit.ly/31OGq3L> [consulta: 06 febrero 2022]
- DONOSO, Lorena. 2011. El problema del tratamiento abusivo de los datos personales en salud. En: Raúl Arrieta Cortés (coord.), Reflexiones sobre el uso y abuso de los datos personales en Chile. [en línea] Santiago, Expansiva <https://bit.ly/3pYMNtw> [consulta: 06 febrero 2022] pp. 79-99
- DONOSO, Lorena. 2016. Protección de datos personales ¿Qué nos piden la OECD y la UE? [en línea] Revista del Colegio de Abogados de Chile, Núm. 66. <https://bit.ly/33eneg4> [consulta: 06 febrero 2022] pp. 25-27.
- ETEROVIC, Pablo. 2019. Acceso a la ficha clínica en el derecho chileno. Ediciones jurídicas de Santiago, Chile.
- HÉRNANDEZ, Héctor. 2001. Tratamiento de la criminalidad informática en el derecho penal chileno: Diagnóstico y propuestas. Informe solicitado por la División Jurídica del Ministerio de Justicia, Santiago. Inédito.
- JIJENA, Renato y REVECO, Rodrigo. 2020. Ciberseguridad y responsabilidades en el sector público. [en línea] Diario Constitucional. 27 diciembre, 2020 <https://bit.ly/3rTwyjT> [consulta: 06 febrero 2022]
- JIJENA, Renato. 2010. Actualidad de la protección de datos personales en América Latina. El caso de Chile. En: [en línea] Memorias del XIV Congreso Iberoamericano de Derecho e Informática. Monterrey: VV.AA. pp. 413-431 <https://bit.ly/3s1Le0c> [consulta: 06 febrero 2022]
- JIJENA, Renato. 2013. Tratamiento de datos personales en el Estado y acceso a la información. [en línea] Revista Chilena de Derecho y Tecnología, Vol. 2, Núm. 2 <https://bit.ly/3oOWifi> [consulta: 06 febrero 2022]
- MAGLIONA, Claudio y LÓPEZ, Macarena. 1999. Delincuencia y fraude informático. Editorial Jurídica de Chile.

- MAYER, Laura y OLIVER, Guillermo. 2020. El delito de fraude informático: concepto y delimitación. [en línea] Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 1, 2020 <https://bit.ly/3ruSWiT> [consulta: 06 febrero 2022]
- MAYER, Laura y VERA, Jaime. 2020. El delito de espionaje informático: concepto y delimitación. [en línea] Revista Chilena de Derecho y Tecnología, Vol. 9, Núm. 2, 2020. <https://bit.ly/3oumyuW> [consulta: 06 febrero 2022]
- VERGARA, Gonzalo. 2018. Institucionalidad en protección de datos personales: Examen de variables regulatorias en el contexto de los proyectos de ley boletines 11.144-07 y 11.092-07 (refundidos). [en línea] Informe solicitado por el H. Senador Kenneth Pugh, Valparaíso <https://bit.ly/3oOw3FK> [consulta: 06 febrero 2022]

- **EXTRANJERA**

- BACHELET, Michelle. 2019. Derechos humanos en la era digital: ¿Pueden marcar la diferencia? [en línea] Discurso Alta Comisionada Derechos Humanos UN, Japan Society, Nueva York <https://bit.ly/2DHu2Xh> [consulta: 06 febrero 2022]
- BENSON, Tim y GRIEVE, Grahame. 2021. Principles of health interoperability: SNOMED CT, HL7 and FHIR. [en línea] Springer International Publishing AG, Suiza. Disponible en PDF en SpringerLink [consulta: 06 febrero 2022]
- BID. 2019. El ABC de la interoperabilidad de los servicios sociales: Guía para los Gobiernos. [en línea] <https://bit.ly/3ERf4In> [consulta: 06 febrero 2022]
- BID. 2019. Interoperabilidad para principiantes: La base de la salud digital. [en línea] <https://bit.ly/3ykerEW> [consulta: 06 febrero 2022]
- BID. 2019. Transformación digital del sector salud en América Latina y el Caribe: La historia clínica electrónica. [en línea] <https://bit.ly/3GDCbXv> [consulta: 06 febrero 2022]
- BRANDEIS, Samuel y WARREN, Louis. 1995. El derecho a la intimidad, Edición de Benigno Pendás y Pilar Baselga. Madrid, Civitas.
- BRAUNSTEIN, Mark. 2018. Health Informatics on FHIR: How HL7's New API is Transforming Healthcare. [en línea] Springer International Publishing AG, Suiza. Disponible en PDF en SpringerLink [consulta: 06 febrero 2022]

- CEPAL. 2007. Libro blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe. [en línea] <https://bit.ly/3pP7ZSE> [consulta: 06 febrero 2022]
- CEPAL. 2021. Gobernanza digital e interoperabilidad gubernamental: una guía para su implementación. [en línea] <https://bit.ly/3pQeCDZ> [consulta: 06 febrero 2022]
- CRIADO, J. Ignacio, GASCÓ, Mila y JIMÉNEZ, Carlos. 2011. Interoperabilidad de Gobierno electrónico en Iberoamérica. Estudio comparativo y recomendaciones de futuro. [en línea] Revista del CLAD Reforma y Democracia, Núm. 50 <https://bit.ly/3IIN1NP> [consulta: 06 febrero 2022]
- GUIJARRO, Luis. 2007. Interoperability frameworks and enterprise architectures in e-government initiatives in Europe and the United States. en línea] Government Information Quarterly, Volume 24, Issue 1 <https://bit.ly/3yjNAZv> [consulta: 06 febrero 2022]
- IBM. 2020. Cost of a Data Breach Report. [en línea] <https://ibm.co/3GzXskU> [consulta: 06 febrero 2022]
- IDIS. 2016. Estudio de interoperabilidad en el sector sanitario: El paciente como actor principal. [en línea] Fundación IDIS, Madrid, España <https://bit.ly/3dI5v2D> [consulta: 06 febrero 2022]
- INSTITUTE OF MEDICINE. 2003. Key Capabilities of an Electronic Health Record System: Letter Report. Washington, DC, EE.UU., National Academies Press En: BID. 2020. Sistemas de Historias Clínicas Electrónicas: Definiciones, evidencias y recomendaciones prácticas para América Latina y el Caribe [en línea] <https://bit.ly/3IJmnnP> [consulta: 06 febrero 2022]
- LEVIATAN Iliona, OBERMAN Berenice, ZIMLICHMAN Eyal, STEIN Gideon. 2021. Associations of physicians' prescribing experience, work hours, and workload with prescription errors. [en línea] Journal of the American Medical Informatics Association, Volume 28, Issue 6 <https://bit.ly/3yu8Rju> [consulta: 06 febrero 2022]
- MINSAIT. 2021. Libro blanco de interoperabilidad en salud. América Latina. [en línea] Edición 2020-2021 <https://bit.ly/3ETSjni> [consulta: 06 febrero 2022]
- MURILLO, Pablo. 2009. La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad. En: Pablo Lucas Murillo de la Cueva y José Luis Piñar. El Derecho a la Autodeterminación Informativa. [en

línea] Madrid, Fundación Coloquio Jurídico Europeo. pp. 11-76. <https://bit.ly/3EPdV4h> [consulta: 06 febrero 2022]

- OMS. 2016. WHO global strategy on people-centered and integrated health services: Interim Report. [en línea] WHO Service Delivery and Safety Department, Ginebra, Suiza <https://bit.ly/3DOloiJ> [consulta: 06 febrero 2022]
- ONU. 2020. Encuesta sobre E-Gobierno, 2020. [en línea] Departamento de Asuntos Económicos y Sociales, Nueva York <https://bit.ly/30kWo51> [consulta: 06 febrero 2022]
- OMS. 2021. Estrategia mundial sobre salud digital 2020-2025. [en línea] Ginebra <https://bit.ly/3pNsfnz> [consulta: 06 febrero 2022]
- PAHO. 2017. Revisión de estándares de interoperabilidad para la eSalud en Latinoamérica y el Caribe. [en línea] PAHO y Oficina Regional para las Américas de la OMS, Washington, D.C., EE.UU. <https://bit.ly/3rZqpTb> [consulta: 06 febrero 2022]
- PEREZ LUÑO, Antonio. 2014. Los derechos humanos hoy: perspectivas y retos. XXII Conferencias Aranguren. [en línea] Revista de Filosofía Moral y Política, Nº 51. <https://bit.ly/3ymvjuU> [consulta: 06 febrero 2022] pp. 465-544
- RACSEL. 2019. Manual estándares interoperabilidad en salud: Recomendaciones técnicas. [en línea] <https://bit.ly/31XElCo> [consulta: 06 febrero 2022]
- ROWLANDS, David. 2020. A Health Interoperability Standards Development, Maintenance and Management Model for Australia. [en línea] <https://bit.ly/31Ce3VT> [consulta: 06 febrero 2022]
- WALKER, Jan, PAN, Eric, JOHNSTON, Douglas, ADLER-MILSTEIN, Julia, BATES, David y MIDDLETON, Blackford. 2005. The Value Of Health Care Information Exchange And Interoperability. [en línea] Health Affairs (Project Hope). Suppl Web Exclusives. W5-10. <https://bit.ly/3GDWe8m> [consulta: 06 febrero 2022]

❖ SENTENCIAS/DICTÁMENES/DECISIONES

➢ Corte Suprema

- Nº 32.059-2014.
- Nº 18.253-2017
- Nº 34.536-2017.

- Nº 31.594-2018.
- Rol Nº 71.906-2020.

➢ **Cortes de Apelaciones**

- Rol Nº 2.584-2017 de la Corte de Apelaciones de Santiago
- Rol Nº 13.251-2019 de la Corte de Apelaciones de Santiago.

➢ **Tribunales civiles**

- Rol Nº 20.855-2014 del 24º Juzgado Civil de Santiago.

➢ **Tribunal Constitucional**

- STC Rol Nº 1.572; STC Rol Nº 1.589; STC Rol Nº 1.629; STC 1.636; STC Rol Nº 1.710; STC Rol Nº 1.745; STC Rol Nº 1.765; STC Rol Nº 1.766; STC Rol Nº 1.769; STC Rol Nº 1.784; STC Rol Nº 1.785; STC Rol Nº 1.806; STC Rol Nº 1.807; STC Rol Nº 976; STC Rol Nº 1.287;STC Rol Nº 2.159.

➢ **CPLT**

- Decisión CPLT Rol Nº C1.511-21; Rol Nº C2.075-16.

➢ **CGR**

- Dictamen CGR Nº 8.113-2020; Nº 52.957-2016; Nº 3.421-2016; Nº 38.604-2013.

➢ **SUPERSALUD**

- Dictamen SUSESO Rol Nº 45.512-2018.

❖ **PROYECTOS DE LEY**

➢ Proyecto de ley que “Consagra el derecho a protección de los datos personales” (boletín Nº 9.384-07) [Ley Nº 21.096]. [en línea] <https://bit.ly/3oNjjz9> [consulta: 06 febrero 2022]

➢ Proyecto de ley que “Establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest” (boletín Nº 12.192-25). [en línea] <https://bit.ly/3Ab5PjL> [consulta: 06 febrero 2022]

➢ Proyecto de ley que “Promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros” (boletín Nº 14.750-05). [en línea] <https://bit.ly/3CWIK6c> [consulta: 06 febrero 2022]

➢ Proyecto de ley que “Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales” (boletín Nº 11.144-07). [en línea] <https://bit.ly/3yoqPTF> [consulta: 06 febrero 2022]

- Proyecto de ley que “Establece medidas para incentivar la protección de los derechos de los consumidores” (boletín 12.409-03). [en línea] <https://bit.ly/3qkuYa0> [consulta: 06 febrero 2022]
- Proyecto de ley sobre “Protección de la vida privada” (boletín Nº 896-07) [Ley Nº 19.628]. [en línea] <https://bit.ly/3m0PVnc> [consulta: 06 febrero 2022]
- Proyecto de ley sobre el “Derecho a optar voluntariamente para recibir asistencia médica con el objeto de acelerar la muerte en caso de enfermedad terminal e incurable” (boletín Nº 7736-11). [en línea] <https://bit.ly/3xmeX2Y> [consulta: 06 febrero 2022]

❖ LEGISLACIÓN EXTRANJERA

- **ALEMANIA**
  - Bundesdatenschutzgesetz. Januar 1977.
- **AUSTRALIA**
  - Australian Privacy Principles. 12 march 2014.
  - My Health Record Act 2012. Compilation No. 9.
  - My Health Records Amendment (Strengthening Privacy) Bill. 2018.
  - My Health Records Rule 2016. Compilation No 1.
  - Privacy Act 1988. Compilation No 89.
- **CANADÁ**
  - Personal Health Information Protection Act (PHIPA). 2004.
  - Personal Information Protection and Electronic Documents Act (PIPEDA). 2004.
  - PIPEDA fair information principles, May 2019.
  - Privacy Act. 1985.
- **ESPAÑA**
  - Carta de Derechos Digitales del Gobierno. 2021.
  - Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. 2002.
  - Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. 1995.
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. 2018.
  - Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter persona. 1992.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica. 2010.
- Real Decreto 69/2015, de 6 de febrero, por el que se regula el Registro de Actividad de Atención Sanitaria Especializada. 2015.

➢ **ESTADOS UNIDOS**

- Health Insurance Portability and Accountability Act (HIPAA). 1996.

➢ **UNIÓN EUROPEA**

- Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Serie de Tratados Europeos – Nº 108. [en línea] <https://bit.ly/3gsgIWt> [consulta: 06 febrero 2022]
- Decisión 1720/1999/CE del Parlamento Europeo y del Consejo de 12 de julio de 1999 por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), así como el acceso a las mismas. [en línea] <https://bit.ly/3dO2Q7K> [consulta: 06 febrero 2022]
- Decisión 2002/2/CE de la Comisión de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos. [en línea] <https://bit.ly/3ERM5Uu> [consulta: 06 febrero 2022]
- Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC). [en línea] <https://bit.ly/31JIWYI> [consulta: 06 febrero 2022]
- Decisión 2012/484/UE de Ejecución de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales. [en línea] <https://bit.ly/3CXxfLP> [consulta: 06 febrero 2022]
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. [en línea] <https://bit.ly/3Gw05DX> [consulta: 06 febrero 2022]
- EIF. 2017. [en línea] <https://bit.ly/2ZXYM0V> [consulta: 06 febrero 2022]

- GDPR. 2016. [en línea] <https://bit.ly/3oP2ROY> [consulta: 06 febrero 2022]

➢ **URUGUAY**

- Decreto Nº 122/019. Reglamentación del art. 194 de la ley 19.670, referente a la incorporación de las instituciones de salud y las personas al sistema de historia clínica electrónica nacional. 13 mayo 2019.
- Decreto Nº 242/017. Reglamentación del art. 466 de la ley 19.355, relativo a los mecanismos de intercambio de información clínica con fines asistenciales a través del sistema de historia clínica electrónica nacional. 7 septiembre 2017.
- Ley Nº 18.331. Protección de datos personales. 18 agosto 2008.
- Ley Nº 18.335. Derechos y Obligaciones de Pacientes y Usuarios de los Servicios de Salud. 26 agosto 2008.

➢ **OTROS**

- CDH. 2021. El derecho a la privacidad en la era digital. Resolución aprobada por el Consejo de Derechos Humanos ONU el 7 de Octubre de 2021, Nº 48/4. [en línea] <https://bit.ly/3s18LP0> [consulta: 06 febrero 2022]
- OCDE. 2002. Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales. [en línea] <https://bit.ly/3kiNaNv> [consulta: 06 febrero 2022]

❖ **TRATADOS INTERNACIONALES**

➢ Carta Europea de Derechos Fundamentales. 2000. [en línea] <https://bit.ly/3rYjCqP> [consulta: 06 febrero 2022]

➢ Convenio de Budapest sobre Ciberdelincuencia. 2001. [en línea] <https://bit.ly/3im7igZ> [consulta: 06 febrero 2022]

➢ Declaración Universal de Derechos Humanos. 1948. [en línea] <https://bit.ly/3ILlHhL> [consulta: 06 febrero 2022]

➢ Pacto Internacional de Derechos Civiles y Políticos. 1966. [en línea] <https://bit.ly/33rQxfl> [consulta: 06 febrero 2022]

❖ **SENTENCIAS EXTRANJERAS**

➢ STJUE

- Rol Nº C-362-14
- Rol Nº C-311-18

➢ URCDP

- Dictamen URCDP Nº 12/018
- Dictamen URCDP Nº 12/021
- Dictamen URCDP Nº 11/021

➢ AEPD

- Procedimiento AEPD Nº PS/00206/2020

❖ **<u>OFICIOS CPLT</u>**

➢ Oficio CPLT Nº 179/2021; 116/2021 58/2021; 43/2021; 157/2021; 868/2020; 748/2020; 746/2020; 675/2020; 1155/2020.

ANEXO. JURISPRUDENCIA RELEVANTE SOBRE FICHAS CLÍNICAS.[291]

A) TRIBUNALES DE JUSTICIA

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
3.645-1997	Protección	Corte de Apelaciones Santiago	**El paciente puede renunciar a la reserva de su información clínica.** "La reserva está establecida en su único y total beneficio y, […] sin lugar a duda es el paciente el titular por excelencia de la información que se resguarda, en cuanto es el llamado por ley a renunciarla o no, según su voluntad, lo que guarda una total coherencia con la institución del secreto profesional".
5.998-2005	Protección	Corte Suprema	**Fonasa cuenta con facultades para revisar fichas de profesionales que fiscalice; se privilegia bien jurídico de la fe pública frente a secreto profesional.** "Fuerza es aceptar que el oficio cuestionado no adolece de ilegalidad, por cuanto el Fondo cuenta con facultades necesarias para realizar la fiscalización […] y tampoco es arbitrario, ya que posee el sustento necesario, en la medida en que su antecedente lo constituye el reclamo de un beneficiario".
6.055-2008	Protección	Corte Suprema	**La solicitud de la ficha por parte del heredero de un paciente fallecido no constituye una violación de la confidencialidad, máxime si se fundamenta en una solicitud racional.** "Parece del todo evidente que no se viola la confidencialidad de la ficha y demás antecedentes médicos que se tengan del paciente fallecido [...], si se entregan a su madre para que ésta pueda cobrar un seguro de vida. No se trata, entonces, de publicar los antecedentes médicos ni entregarlos a cualquier persona que los solicita".

[291] Agradecimientos al profesor Luis Cordero Vega por sus periódicas publicaciones jurisprudenciales en redes sociales, muchas de las cuales están incluidas en el presente.

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
1.781-2010	Protección	Corte de Apelaciones Santiago	**La negativa del prestador de rectificar los datos de la ficha del titular vulnera su derecho a la privacidad y a la propiedad de sus datos.** "Esta Corte no divisa razón alguna, legal ni reglamentaria, que legitime la posición adoptada por la recurrida de negarse a efectuar la rectificación del nombre del paciente menor de edad en la ficha respectiva, más aún si se considera que el que consta en ésta ya no existe, no puede seguir usándose"
1.226-2011	Protección	Corte de Apelaciones Concepción	**La negativa a entregar la ficha clínica al titular constituye un acto ilegal que vulnera sus derechos a la vida, a la integridad física y psíquica, y de propiedad.** "El recurrente tiene derecho a la información […] por así disponerlo el art. 12 [Ley 19.628] y según el art. 13, el derecho de las personas a la información de sus datos no puede ser limitado por medio de ningún acto o convención […] el recurrente tiene derecho a la información del contenido de su ficha […], que solicita de la recurrida". (También, de la misma Corte, Rol 1.191-2011 y 1.057-2011)
32.059-2011	Protección	Corte Suprema	**No corresponde exigir posesión efectiva para que un hijo acceda a la ficha de su padre fallecido.** "La posesión efectiva de la herencia es un trámite de orden procesal que deben hacer uno o más de los herederos […] para poder disponer legalmente de los bienes dejados por el causante. Entonces, este trámite no tiene relación con el que ha dado motivo a interponer la acción".
29.221-2015	Demanda ind. perjuicios	16º Civil de Santiago	**Condena a persona jurídica a indemnizar a tres de sus clientes por haber tratado indebidamente sus datos personales por infracción a los artículos 6 y 11 LPVP, debiendo pagar dos millones a cada uno de los actores por concepto de daño moral.** La demanda fue motivada por el hallazgo, en octubre del año 2015, de documentos abandonados en un basural clandestino que

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
			contenían información de un grupo de clientes del demandado. Según se indicó en la presentación, en los documentos se encontraron copias de cédulas de identidad, estados de situación financiera, evaluaciones crediticias, liquidaciones de sueldo, cheques personales y de terceros, información sobre dineros en cuentas personales, entre otros. Los demandantes reclamaron una infracción a los artículos 6 y 11 de la LPD, y un daño que el demandado, en su calidad de responsable del banco de datos, debía reparar íntegramente. En cuanto al daño moral, la demanda sostuvo que los hechos acontecidos provocaron dolor, molestia, angustia y aflicción en los titulares de los datos al verlos expuestos por una entidad en la que ellos habían depositado su confianza. El abandono de los documentos, continuaron, implicó que cualquiera podría haber conseguido información privada, poniendo en riesgo -según los demandantes- su seguridad y la de sus familias. En virtud de esto, avaluaron los demandantes su daño moral en veinticinco millones de pesos para cada uno de ellos. "Las partes demandantes vieron vulnerada su confianza depositada en (el demandado), quien no cuidó con la debida diligencia los datos personales y sensibles que de ellos obtuvo. Por eso, se inició una serie de actos que terminó con los datos de estas personas absolutamente expuestos y vulnerables ante terceros, y es dable concluir que por ello, según sus alegaciones y pruebas aportadas, esta situación les causó gran trastorno moral, preocupación e incluso angustia, durante el período de tiempo que duraron estas circunstancias e incluso después, por la sensación de inseguridad producida, por lo que se accederá a la demanda".
2.584-2017	Demanda ind. perjuicios	Corte Apelaciones de Santiago	**Constituye negligencia médica y falta de servicio el extravío de fichas clínicas de una paciente que fue dada de alta a pesar de**

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
			presentar daño hepático (condenan por daño moral 25 millones)
20.855-2017	Demanda ind. perjuicios	24º Civil de Santiago	**La divulgación, manipulación y tratamiento ilegal de datos de un paciente, considerados sensibles por referirse a su atención médica, por parte de funcionarios del prestador genera daño moral tanto por las normas de la ley 20.285 (arts. 12 y 13) y 19.628 (arts. 4, 5, 9, 10 y 12), relacionado con el tratamiento y cuidado indebido de datos sensibles y su difusión por personas no autorizadas.** "Independiente de la existencia de protocolos y manuales con que cuenta la demandada para el tratamiento de datos personales sensibles de sus pacientes, se vulneraron sus protocolos por una funcionaria de dicha entidad, y por tanto, no se trataron y divulgaron los datos sensibles de la paciente, contenidos en su ficha clínica, de conformidad a la Ley, haciéndolos públicos a terceros, sin una razón legal o justificada." "De hecho, conforme por lo reconocido por uno de los testigos presentados por la propia demandada, puede advertirse que dicha institución no ha considerado en sus protocolos el tratamiento de datos sensibles a través del acceso por otras vías, como es la información vinculada con el sistema financiero contable, y que permite acceso de igual forma a los datos sensibles de los pacientes."
38.666-2017	Protección	Corte Suprema	**Empresa no puede condicionar el acceso a datos personales propios a un pago, pues se afecta el derecho personalísimo del titular de los mismos.**
1209-2018	Protección	Corte Suprema	**Ley de datos personales no se aplica a personas jurídicas. Votos en contra ministros Prado y Aranguiz. (En el pasado reciente la CS había sostenido una tesis contraria también en votaciones divididas, ver roles 27.889 y 37301-2017; 961-2018). En sentido contrario (es decir, que se aplica la ley de datos personales a personas**

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
			jurídicas) ha resuelto en casos roles 961-2018 (22.3.2018), 27889-2017 (30.10.2017) y 37.301-2017 (24.10.2017).
6.563-2018	Protección	Corte Suprema	**La negación de una clínica privada de hacer entrega de la ficha clínica a un tercero previamente autorizado por el titular vulnera el derecho de propiedad.** Es decir, un tercero aparece debidamente autorizado por su titular para obtener la información de la ficha cínica, pues las actuaciones que se le encargan (como abogado) suponen la obtención de la información que se le niega.
56.593-2018	Protección	Corte de Apelaciones de Santiago	**La negativa de hacer entrega de la ficha clínica a un paciente con deudas pendientes con el centro de salud por hospitalización en circunstancias en que era menor de edad atenta contra el derecho de propiedad.**
18.253-2018	Casación	Corte Suprema	**Acoge casación en el fondo en caso de demandante que no fue notificado oportunamente de examen de VIH positivo. Se verifica la falta de servicio por la no entrega de los resultados del examen en forma oportuna y por existir un diagnóstico errado. La dilación en el resultado generó que otras personas también se contagiaran. Hospital señala que la información de la ficha clínica estaba incompleta y desactualizada, lo cual no fue óbice para eximirse de la falta de servicio. Sentencia de reemplazo otorga 25.000.000 pesos por daño moral debido a que "Habiéndose practicado el examen de VIH el 1 de octubre de 2007, sin que nadie le comunicará de sus resultados, enterándose finalmente a través de un examen particular sólo a partir del 13 de abril de 2010".**
35.292-2020	Protección	Corte de Apelaciones de Valparaíso	**Resulta razonable que las recurridas, en atención a que prestan funciones de salud de manera interrelacionadas y en un mismo lugar físico, mantengan una ficha única en beneficio de los pacientes que se atienden**

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
			en el lugar; antecedentes que, por lo demás, no fue compartidos con terceros ajenos a los tratamientos de salud requeridos. Por lo mismo, no puede prosperar una petición de destrucción de la ficha teniendo presente el art. 11 del Decreto Nº 41 MINSAL. **Sin embargo, negar o demorar la entrega de exámenes médicos implica una privación de bienes de propiedad del paciente que le sirven para continuar su tratamiento de salud, afectando, en consecuencia, los artículos 19 N°1 y 24 de la CPR.**
21.137-2020	Protección	Corte Suprema	**FONASA no puede acceder a fichas clínicas para los efectos de comprobar si 200 pacientes han sido atendidos por un determinado médico. Las funciones médico-administrativas le corresponden a la respectiva COMPIN.** "Que, conforme se colige de las disposiciones antes citadas, FONASA y las Secretarías Regionales Ministeriales tienen asignadas funciones que se complementan entre sí, en tanto a la primera le corresponden las de orden administrativo y financiero, a la segunda las médico administrativas que se ejecutan mediante las respectivas COMPIN. Establecido lo anterior, si lo que se quiere verificar por la recurrida, para efectos de cuidar que el financiamiento que efectué corresponda a las prestaciones otorgadas a sus beneficiarios, es la real condición de salud de los pacientes y la justificación de las acciones de salud que ha debido financiar, basta con que la COMPIN, en el ejercicio de las facultades técnicas complementarias a las de la recurrida, disponga la práctica de los exámenes y actuaciones clínicas necesarias para dilucidar lo anterior, valiéndose al efecto de todos aquellos registros que aquélla debe tener, en relación a cada paciente, de las prestaciones de salud recibidas, actuar que torna prescindible la revisión de las fichas clínicas de éstos."

ROL	RECURSO	TRIBUNAL	RESEÑA PRINCIPAL
10.532-2020	Protección	Corte de Apelaciones de San Miguel	**Un requisito esencial para que prospere una acción de protección es la existencia de un derecho indubitado. En consecuencia, no es posible satisfacer la pretensión de una hija que solicita a un centro médico la ficha clínica de su padre fallecido, al no constar registro de la ficha ni tampoco de una atención médica.** "[…] puede concluirse que la materia planteada no es susceptible de ser solucionada por la presente vía, esto es, la acción cautelar de derechos constitucionales, particularmente porque la recurrente no es titular de un derecho indiscutido o indubitado, desde que no se encuentra acreditada la existencia de los antecedentes médicos cuya entrega pretende". […] una controversia así generada, no puede ser dilucidada por medio de la presente acción cautelar de derechos constitucionales, ya que esta no constituye una instancia de declaración de tales derechos, sino que de protección de aquellos que, siendo preexistentes e indubitados, se encuentren afectados por alguna acción u omisión ilegal o arbitraria, por lo que la acción intentada no puede prosperar."
13.251-2020	Habeas Data	Corte Apelaciones Santiago	**Se condena a un perito contratado para informar a un tribunal de familia a hacer entrega de todos los resultados obtenidos de los exámenes al titular de estos.**
38.554-2021	Protección	Corte Suprema	**Es ilegal sanción impuesta por Fonasa a un médico que se negó a entregar las fichas clínicas de sus pacientes para efectos de fiscalización. El facultativo tiene la prohibición de divulgar los datos sensibles de sus pacientes sin autorización expresa**
49.701-2021	Protección	Corte Suprema	**Fonasa no puede requerir copia de fichas clínicas para ejercer su fiscalización, pues estas se encuentran protegidas. La autoridad dispone de otros medios para verificar la procedencia de los diagnósticos médicos que desea controlar** (También Rol Nº 49.703)

B) CONTRALORÍA GENERAL DE LA REPÚBLICA.

DICTAMEN	RESEÑA PRINCIPAL
21.413-1984 y 24.238-2010	Solo pueden tener acceso a la ficha aquellos funcionarios que desempeñan funciones habituales de acceso dentro de su respectivo cargo. "Misma sanción expulsiva corresponde a otra funcionaria de ese hospital que […] ingresó a la sala en que acababa de fallecer otra paciente, ubicada al lado de la anterior, donde examinaron la ficha que creyeron pertenecía a ésta, no pudiendo explicar a las autoridades del hospital esta actitud, puesto que todo ello no estaba dentro de las actividades habituales que les correspondía desempeñar dentro de sus respectivos cargos".
36.049-1995 y 9.642-2003	**Procede remitir fichas requeridas por Cámara de Diputados.** "El Ministerio de Salud debe remitir fichas requeridas por la Cámara de Diputados, en la forma prevista en Ley 18.918 […] para proporcionar los documentos secretos o reservados por su naturaleza o en virtud de una disposición especial que no tiene fuerza de ley".
10.808-1998 y 30.822-1998	**Los acuerdos entre hospitales y empresas de servicios que permiten a terceros (empresas) tomar conocimiento de la información contenida en las fichas, resultan objetables y afectan su reserva.** "Resultan objetables las cláusulas del acuerdo [entre hospital y empresa de servicios] que permiten a terceros (empresas) tomar conocimiento de información contenida en fichas del hospital, aun cuando exista un pacto entre las partes para que la sociedad contratante guarde estricta reserva de los datos consignados en los aludidos documentos. Esto, por cuanto la ley prohíbe a funcionarios de la administración del Estado divulgar hechos relativos a personas o entidades, que hayan conocido en el desempeño de sus actividades".
47.022-2000 y 72.962-2009	**Hospitales no pueden negarse a proporcionar información de fichas clínicas a sus titulares o representantes.** "La información clínica que afecta a personas tendrá carácter reservada y solo se podrá entregar a los Tribunales u otras entidades legalmente autorizadas para requerirla, [la] que solamente podrá proporcionar información a otras instituciones con la conformidad del paciente. […] Los hospitales dependientes de los Servicios de Salud no pueden negarse a proporcionar la información contenida en las fichas a las personas a que éstas se refieren o a sus representantes".
47.022-2000	**Pacientes pueden ejercer el denominado Habeas Data respecto de organismos que efectúen un tratamiento de los datos de sus fichas.** "En lo que se refiere a Ley 19.628 es útil consignar que en aquellos casos en que la autoridad efectúe tratamiento de datos en registros o bancos de datos respecto de la información contenida en las fichas […]

DICTAMEN	RESEÑA PRINCIPAL
	el titular de los datos […] tiene derecho a exigir a quien sea responsable del banco, información sobre los datos relativos a su persona".
8.531-2001 y 52.739-2005	**Fonasa tiene facultades para revisar fichas de beneficiarios.** "Se encuentra en el deber de fiscalizar la modalidad de libre elección […], y que en cumplimiento de esa función cuenta con atribuciones para exigir a los profesionales o entidades inscritos […], la presentación de toda la información técnica o administrativa que respalde el otorgamiento de las prestaciones […], incluida aquella de carácter reservado que se contenga en fichas".
71.601-2009	**La ficha solicitada a un centro sanitario solo puede ser proporcionada sin el consentimiento del titular, para determinación de beneficios de salud.** "Las fichas solicitadas por la Comisión de Sanidad Fuerza Aérea de Chile, por incidir en el estado de salud de las personas, contienen datos sensibles […], por lo que solo pueden ser proporcionadas sin el consentimiento de los afectados, cuando ellas sean necesarias para la determinación de beneficios de salud para los mismos".
74.968-2012	**Información sobre el estado de salud constituye un dato reservado que debe ser resguardado durante toda la atención al paciente.** "[El solicitante] añade, que durante su atención en el citado establecimiento la referida funcionaria gritó a viva voz, frente al resto de los funcionarios y pacientes, el procedimiento médico que se aplicaría al recurrente, el medicamento que se le había prescrito y la enfermedad a la que éste estaba destinado […]. Se debe consignar que el art. 12 de la citada ley [20.584], dispone que toda la información que surja […] será considerada como dato personal sensible".
84.748-2013	**La Intendencia de Prestadores de la Superintendencia de Salud puede requerir la ficha a un prestador.** "La mencionada autoridad de fiscalización sectorial se encuentra habilitada para recabar los antecedentes respecto a los hechos investigados que le servirán para determinar si efectivamente la paciente se encontraba en la situación de emergencia o urgencia, a que hace alusión el artículo 141 del Decreto con Fuerza de Ley N°1, de 2005, y precisar también en qué momento fue estabilizada".
86.382-2013	**Funcionarios de Contraloría detentan atribuciones para revisar fichas de pacientes atendidos en los servicios.** "Los órganos sujetos al control y fiscalización […] están obligados a entregar a [la Contraloría] toda información o documento que se encuentre en su poder, en la medida que ello sea necesario para el debido ejercicio de las funciones que la Constitución y la ley le confieren, puesto que esta Entidad de Control es uno de aquellos organismos habilitados por el ordenamiento jurídico para acceder a los datos contenidos en esas fichas".

DICTAMEN	RESEÑA PRINCIPAL
38.604-2013	**Si bien la ley N° 20.584 dispuso su conocimiento por los funcionarios y entidades enumeradas expresamente en su artículo 13, debe tenerse presente que las disposiciones de dicho artículo destinadas a evitar la intromisión de terceros no vinculados con el paciente en la ficha clínica de éste, no han alterado otras prescripciones legales que autorizan a determinados funcionarios o entidades para realizar el tratamiento de tales fichas.** Así, sobre la base de las referidas consideraciones, procede aplicar el artículo 13 de la ley N° 20.584 en forma complementaria a la ley N° 19.628 y a los demás preceptos legales vigentes, con el fin de que toda esta normativa produzca sus efectos y se protejan correctamente los derechos de los beneficiarios (aplica dictamen N° 19.652, de 2013). Sobre la confidencialidad de los antecedentes médicos de los internos de los establecimientos penitenciarios concesionados.
19.652-2013	**Se encuentran autorizados para acceder a la ficha clínica de un paciente, además de las personas y organismos indicados en el artículo 13 de la ley Nº 20.584, aquellos que hayan sido habilitados por otros cuerpos legales.** Lo anterior puesto que el artículo 10 de la ley Nº 19.628 permite que los datos sensibles sean objeto de tratamiento, cuando la ley lo autorice, exista consentimiento del titular o sean necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares, situaciones que se configuran respecto de diferentes entidades, tales como el Ministerio de Salud, la Superintendencia de Salud y su Intendencia de Prestadores de Salud, y el Fondo Nacional de Salud, entre otras, todas ellas autorizadas, como ha podido apreciarse, mediante el aludido decreto con fuerza de ley Nº 1, de 2005. “Las entidades acreditadoras están facultadas para acceder a la ficha, dado que el art.10 de la Ley 19.628 permite el tratamiento de los datos sensibles cuando ‘la ley lo autorice’, situación que en este caso tiene como fundamento el Decreto con Fuerza de Ley N° 1, de 2005 [que crea] un sistema de acreditación de prestadores”.
84.748-2013	**La Intendencia de Prestadores de Salud ha obrado conforme a derecho, al requerir la aludida información, pues aun cuando sea un tercero quien haya solicitado se inicie un proceso de investigación, esa entidad, con los alcances expuestos, se encuentra facultada para solicitar tales documentos, en atención a las competencias brindadas por la normativa reseñada.** “Si bien el artículo 12 de la mencionada ley N° 20.584 prescribe que la información contenida en la ficha clínica es considerada dato sensible y está sujeta al deber de reserva, por parte del prestador respectivo, ello no impide que la Intendencia del ramo pueda requerir los antecedentes necesarios, tendientes a poder ejercer las labores de fiscalización que

DICTAMEN	RESEÑA PRINCIPAL
	le ha encomendado el ordenamiento jurídico, tal como ha reconocido esta Contraloría General en el dictamen N° 19.652, de 2013. Lo anterior, con todo, no importa eximir a la Intendencia de Prestadores de Salud de adoptar los resguardos contemplados en los artículos 7°, 9°, y 20 de la citada ley N° 19.628, impidiendo que terceros no habilitados puedan acceder a esa documentación.”
322-2014	**Fiscal de un procedimiento sumario administrativo se encuentra habilitado para requerir una ficha.** “En tales condiciones, no ha procedido que el Centro de Salud Familiar requerido se haya negado a la entrega de la información solicitada, justificando su respuesta en la citada Ley 20.584, puesto que […] el sumariante se encuentra habilitado para requerir dicha información en el contexto de la investigación ordenada llevar a cabo”.
3.421-2016	**Los antecedentes contenidos en una ficha clínica constituyen datos sensibles cuyo acceso sólo está permitido en los casos previstos por la ley.** “La Contraloría Regional de Valparaíso ha remitido la presentación de don Jaime Vidal Figueroa, médico cirujano del Hospital Naval Almirante Nef, quien consulta sobre la procedencia jurídica de que el comité ético científico de ese centro de salud, constituido en el marco de la ley N° 20.120 -sobre la investigación científica en el ser humano, su genoma, y prohíbe la clonación humana-, apruebe “investigaciones científicas retrospectivas”, en las que los respectivos científicos necesiten utilizar datos biomédicos anónimos obtenidos de las fichas clínicas de pacientes, sin contar con el consentimiento de estos.”
52.957-2016	**La autoridad administrativa, en el nivel jerárquico de que se trate, debe establecer y hacer efectiva la responsabilidad administrativa de los funcionarios que han permitido que las bases de datos que contienen información sensible de los usuarios de los establecimientos de salud, fuesen transmitidas al personal de unidades que, en razón de sus funciones, no está habilitado para acceder a las mismas, dado que dicha divulgación no se encuentra permitida por la normativa** (aplica Nº 3.421 de 2016). Lo anterior, sin perjuicio, además, de la determinación del eventual incumplimiento contractual por parte del proveedor de los servicios informáticos y la consiguiente aplicación de las medidas que el convenio contemple, en el caso de haberse omitido la protección que la preceptiva otorga al tratamiento de la información comentada. Ello, en el contexto de una falla de seguridad del sistema informático del MINSAL que permitió que desde cualquier computador o servidor de esa secretaría de Estado, de los Servicios de Salud y de los establecimientos de atención primaria de salud municipal, se accediera,

DICTAMEN	RESEÑA PRINCIPAL
	sin ninguna clave, a carpetas compartidas que contenían datos sensibles de pacientes.
29.921-2017	**Ficha clínica puede ser requerida para acceder a un beneficio previa autorización del interesado** Se solicitó un pronunciamiento a la Contraloría General de la República –por parte de un funcionario de la Dirección de Aeronáutica Civil (DAC)- para que determine si la Comisión de Sanidad de la Fuerza Aérea debe, necesariamente, acceder a su ficha clínica para emitir su informe respecto de si la enfermedad que lo aquejó es de origen laboral.
9.400-2020	**Antecedentes médicos tienen la calidad de datos sensibles. Resulta inoficioso pronunciarse sobre la legalidad de oficios de la Superintendencia de Pensiones que fueron dejados sin efecto.** “Mediante esas instrucciones se habría facultado a las AFP para requerir y disponer de datos sensibles de los afiliados durante la tramitación de solicitudes de pensión de invalidez, lo cual, habría implicado una vulneración a las normas relativas a la protección de la vida privada.”
8.113-2020	**No procede la entrega de datos sensibles de salud relativos al diagnóstico de pacientes COVID-19, a las municipalidades.** “La información de salud relativa a los pacientes que hayan sido diagnosticados con COVID-19, forma parte de la ficha clínica de cada uno de ellos y, en consecuencia, constituye un dato sensible que solo puede ser objeto de tratamiento -esto es, puede ser extraído, disociado, comunicado, cedido, transferido, transmitido o utilizado en cualquier otra forma-, en lo que interesa, cuando la ley lo autoriza expresamente (aplica criterio contenido en el dictamen Nº 52.957, de 2016). En este orden de ideas, cumple con señalar que el artículo 13 de la referida ley Nº 20.584, establece que los terceros que no estén directamente relacionados con la atención de salud de la persona no tendrán acceso a la información contenida en la respectiva ficha clínica, lo que se extiende, incluso, al personal de salud y administrativo del mismo prestador que no esté vinculado a su atención. Así las cosas, “no resulta procedente la entrega a tales entidades o autoridades de información de salud relativa a los pacientes que hayan sido diagnosticados con el denominado COVID-19, sin su consentimiento. Cualquier medida en contrario requerirá de la aprobación de la correspondiente ley modificatoria que así lo permita.”
7.934-2020	**SENDA puede celebrar convenios con los organismos que indica para la entrega de datos relacionados con las atenciones de salud otorgadas a los beneficiarios de los programas que ejecuta.** “[…] siempre que en las estipulaciones de los mismos se deje expresamente establecido que los respectivos datos podrán ser utilizados solo para los fines señalados en el artículo 10 de la ley N°

DICTAMEN	RESEÑA PRINCIPAL
	19.628 y ser conocidos únicamente por las personas mencionadas en el inciso segundo del artículo 13 de la ley N° 20.584.
9.545-2020	**No se advierte inconveniente que se implemente, en las ambulancias del SAMU, el acceso al sistema de identificación biométrica mediante huella dactilar**, "[…] siempre que los respectivos datos se utilicen solo para los fines señalados en el artículo 10 de la ley N° 19.628 y sean conocidos únicamente por las personas mencionadas en el inciso segundo del artículo 13 de la ley N° 20.584 (aplica dictamen N° 7.934, de 2020, de este origen).
65.938-2021	**No se advierte inconveniente jurídico en que la SUSESO pueda requerir al Instituto de Seguridad del Trabajo (IST) el acceso remoto a sus sistemas informáticos de atención de pacientes en los casos que determine a través de sus instrucciones, adoptando las medidas necesarias para el resguardo de la confidencialidad de la información sensible involucrada.** "En particular, en cuanto a la referida facultad de la SUSESO para requerir el acceso a información -a la que alude el IST-, es necesario precisar que el legislador no distingue si tal acceso es presencial o remoto, por lo que no corresponde excluir esta última posibilidad […]" "Lo anterior, sin perjuicio de lo dispuesto en el inciso final del artículo 56 de la ley N° 20.255, en concordancia con el artículo 2°, letra g), párrafo final, de la ley N° 16.395, en cuanto al deber del personal de la SUSESO de guardar reserva y secreto absolutos de las informaciones de las cuales tome conocimiento en el cumplimiento de sus labores, en las condiciones que indican esos preceptos."

C) CONSEJO PARA LA TRANSPARENCIA.

DECISÓN	RESEÑA PRINCIPAL
C533-09 y C1.796-12	**Los solicitantes no tienen acceso a licencias médicas o datos de salud de terceros.** "En relación con los motivos del otorgamiento de tales licencias [médicas] este Consejo estima que no debe entregarse dicha información por referirse a estados de salud de las personas, en conformidad con el art. 2°, letra g), de la Ley 19.628".
C759-10 y C529-13	**El derecho de acceso a la información pública cuando el dato personal (ficha clínica) obra en poder de un organismo, se comprende como ejercicio del derecho del art. 12 de la Ley 19.628 o habeas data impropio.**

DECISÓN	RESEÑA PRINCIPAL
	"La información […] se enmarca dentro de lo que la Ley 19.628 define en su art. 2°, letra f), como datos personales […] al haber requerido su titular dichos antecedentes al órgano reclamado, utilizando el procedimiento administrativo de acceso a la información, ha ejercido una de las prerrogativas que le confiere el art. 12 […], conocido como el derecho de acceso a la información del titular de los respectivos datos personales, comprendido dentro de lo que se denomina habeas data impropio".
C418-10	**El consentimiento que debe prestar el titular para la cesión de sus datos debe ser informado, expreso, por escrito y específico.** "El consentimiento que debe prestar el titular de datos para la comunicación o cesión de sus datos debe, al menos, ser informado, expreso, por escrito y específico, para la finalidad que se indique. La especificidad debe estar referida a la indicación expresa de los datos o documentos que se autoriza tratar, en la especie, ceder o recolectar".
C920-10 y C475-12	**La representación de un menor en la solicitud de acceso a su ficha corresponde a sus padres de conformidad a las reglas generales del derecho común.** "La titularidad de los datos sensibles corresponde a un menor de edad, habiendo formulado la solicitud de acceso quien ha acreditado tener la filiación materna del menor, a lo cual ha asentido también su padre, con lo que se ha entendido que existe habilitación para requerir dicha información".
C920-10 y C732-12	**Los organismos podrán entregar copias autorizadas de las fichas que les soliciten, así como también desglosar sus antecedentes y en orden cronológico.** "En cuanto al desglose a cargo de personal calificado, este Consejo estima que deberá procederse a la entrega de esta forma, dado que a su respecto la reclamada ha manifestado su plena disposición, por lo demás dicha solución se enmarca en el principio de facilitación"
C322-10 y C372-13	**Si bien una persona fallecida no es titular de datos personales, sus familiares sí pueden acceder a tales datos (ficha o autopsia) para resguardar el honor que se proyecta como propio de estos u otros derechos.** "Aceptar la confidencialidad absoluta de la ficha de un fallecido impediría el acceso a los antecedentes que pudieran revelar la existencia de eventuales negligencias médicas y ejercer el derecho a perseguir las responsabilidades civiles y penales, si fuera el caso, como también el ejercicio de otros derechos (ej. relativos a un seguro de vida)".
C556-10 y C58-13	**Para que un familiar acceda a la ficha de un paciente fallecido, debe acreditar: a) ser heredero según art. 983 Código Civil, o actuar en su representación; b) tener una legitimación activa para ejercer otros derechos que supongan el acceso previo.**

DECISÓN	RESEÑA PRINCIPAL
	"Si bien la información contenida en documentos tales como las fichas ya no sean 'datos personales', sino simples 'datos', por referirse a una persona ya fallecida, este Consejo estima que su tratamiento podría afectar derechos de sus familiares, como un derecho propio de éstos […]. Su revelación podría causarles perjuicios difíciles de evaluar, por lo que se trata de información reservada cuya comunicación puede realizarse en ciertas ocasiones y bajo ciertas circunstancias".
C322-10 y C372-13	**Las auditorías son públicas, debiendo resguardarse los datos personales.** "En relación a auditorías internas, éstas son, en principio, públicas, debiendo el organismo público […] resguardar los datos personales que provengan o hubieren sido recolectados de fuentes no accesibles al público o los datos sensibles que pudiere contener, en consonancia con el principio de divisibilidad […]".
C1.586-12	**La entrega de la ficha debe ser completa; no procede aplicar principio de divisibilidad.** "Tampoco resulta procedente exigir a la requirente que indique el rango de fechas en relación con el cual pide antecedentes de la ficha, o señale las partes específicas de la misma a que pretende acceder, pues […] la solicitud se dirige a la ficha completa".
C1.586-12	**La entrega de la ficha bajo la Ley 20.584 no exige otros requisitos adicionales a los que establece la norma; no requiere expresar motivos.** "La ficha requerida corresponde a una persona que se encuentra fallecida, habiendo sido requerida por quien posee la calidad de hija de la misma, y que por lo mismo debe estimarse heredera legitimaria al tenor de lo prescrito en el art. 1182 Nº 1 Código Civil. De este modo, la reclamada se encuentra plenamente habilitada para acceder [a ella]".
C923-12	**Los procedimientos y gestiones de notificación de exámenes VIH contenidos en las fichas son públicos, debiendo entregarse dicha información al tercero solicitante resguardando la identidad de los titulares.** "Resulta posible, en todo caso, aplicar el principio de divisibilidad, pudiendo entregarse aquella parte de una ficha que contenga tal información, sin hacer referencia a la identidad de su titular u otro antecedente que permita identificarlo, resguardando los datos […] de sus titulares".
2.075-16	**Sobre la base de que un adecuado proceso de anonimización elimina la posibilidad de determinar la identidad de una persona a través del cruce con información que circula libremente en internet, el CPLT ordena a la Superintendencia de Salud que haga entrega de información —amplia— de contratos de salud, cotizantes y cargas de isapre, prestaciones de salud, egresos hospitalarios, licencias**

DECISÓN	RESEÑA PRINCIPAL
	médicas y subsidios por incapacidad y cotizaciones de salud, debiendo tarjar los antecedentes que para cada caso se indica.
C1.511-21	**Se rechaza el amparo deducido en contra de la Policía de Investigaciones de Chile, referido a 22 informes técnicos emitidos por la Comisión Médica de la PDI con todos sus antecedentes, mediante los cuales se otorgó la jubilación por invalidez de segunda categoría por patologías mentales a dichos funcionarios. Lo anterior, por estimar que el acceso a los antecedentes en los términos requeridos importa un riesgo de divulgación de información de carácter altamente sensibles de sus titulares, cuya divulgación producirá una afectación específica a la esfera de la vida privada de aquellos.**

D) SUSESO.

ROL	RESEÑA PRINCIPAL
11.152-2012	**Recae en el empleador la obligación de informar a sus trabajadores acerca de los posibles riesgos que entrañen sus labores, para lo cual no es menester que tenga conocimiento de la información sensible de su estado de salud, ya que con los exámenes preocupacionales y ocupacionales se determinará si un trabajador se encuentra apto o no para desarrollar un determinado quehacer laboral.** A fin de que el empleador pueda dar cumplimiento el Deber de Higiene y Seguridad contemplado en el citado artículo 184 del Código del Trabajo, se complementa el Oficio N°6201 de Concordancias, precisando que los organismos administradores de la Ley N°16.744 pueden entregar a sus empresas cotizantes o adherentes información respecto de las limitaciones físicas o psíquicas de sus trabajadores (por ejemplo, indicar zona o segmento dañado) sólo en tanto esta información se traduzca en indicar la aptitud del trabajador para desempeñar una labor determinada, o especificar los tipos y condiciones de trabajo que, temporaria o permanentemente, estén contraindicados sin dar a conocer los diagnósticos y con las indicaciones médicas correspondientes sobre el reintegro laboral de los accidentados o enfermos profesionales y cambios de faena cuando proceda, todo ello orientado a proteger eficazmente la vida y salud de los trabajadores. Se reitera, además, que no se puede dar a conocer el resultado de exámenes médicos sin la autorización expresa del paciente.
51.927-2013	**La información contenida en la ficha, copia de la misma, o parte de ella, podrá ser entregada, total o parcialmente, a un tercero debidamente autorizado por el titular, mediante poder simple otorgado ante notario.**
49.749-2013	**La actuación de esa Mutualidad en relación con la eliminación de los antecedentes médicos del trabajador no se ha ajustado a lo que en otras**

ROL	RESEÑA PRINCIPAL
	ocasiones ha referido este Servicio (v.gr. Ords. N°s. 7.765, de 1988; 14.141, de 1992; 31.661, de 2003). "En efecto, el D.L. Nº 2.412, de 1978, establece en su artículo 2, que las Instituciones de Previsión podrán microfilmar o reproducir electromagnéticamente la documentación entregada a su custodia. Agrega la norma que con la misma autorización pueden destruir los originales una vez que hayan sido microfilmados o reproducidos y que los documentos microfilmados o reproducidos y sus copias, debidamente autorizados, tendrán el mismo valor probatorio que los originales." "Corresponde que esa mutualidad efectúe las correcciones procedimentales que le permitan evitar contingencias como las referidas, manteniendo el debido respaldo de los antecedentes médicos de los beneficiarios de la Ley N° 16.744."
43.630-2016	**Los organismos administradores deben informar los resultados de los exámenes practicados a los trabajadores en razón de la vigilancia epidemiológica, en forma agregada e innominada, dando las indicaciones para que la empresa realice las acciones para la prevención de las enfermedades profesionales que pudiesen presentarse**. Distinta es la situación de aquel trabajador ya diagnosticado que debe ser trasladado de puesto de trabajo, ya que en tal caso los organismos administradores deben individualizarlo, así como deben informar el agente de riesgo a que se encontraba expuesto, con el fin de que sea trasladado a otro puesto de trabajo o faena donde el referido agente no esté presente, todo ello, sin dar a conocer el diagnóstico ni los resultados de los exámenes específicos de dicho trabajador.
45.512-2018.	**Las mutualidades de empleadores, en su carácter de organismos administradores del Seguro Social de la Ley N° 16.744, se encuentran legalmente habilitadas para acceder a la información contenida en las fichas clínicas de los trabajadores de sus empresas adherentes o afiliadas, tanto cuando les brinden atención médica en sus propios centros médicos, como cuando los deriven a sus prestadores médicos en convenio.** "El cumplimiento de todas y cada una de funciones u obligaciones que las mutualidades deben ejecutar o cumplir conforme al ordenamiento jurídico vigente, suponen como condición esencial e ineludible, el acceso y tratamiento de los datos sensibles contenidos en la ficha clínica, con el objetivo de evaluar y determinar, en primer lugar, mediante el proceso de calificación, la existencia de un accidente del trabajo o de una enfermedad profesional que torne procedente la cobertura del Seguro de la Ley N°16.744, y en caso afirmativo, las prestaciones médicas que el trabajador requiere para su recuperación, de acuerdo al tipo de diagnóstico, su evolución y la existencia o no de incapacidad temporal o permanente, entre otros factores.

ROL	RESEÑA PRINCIPAL
26.481-2019	**Se instruye a la Mutualidad, para que entregue al interesado la información contenida en su ficha clínica y resultados de los exámenes médicos que le realizaron**
2.753-2020	**La obtención, a través de un llamado telefónico, del acuse recibo del paciente de las indicaciones médicas y administrativas otorgadas con posterioridad a una atención vía telemedicina, cumple con las exigencias y objetivos expresados en el Oficio N°1.222, bajo condición que dicho llamado se efectúe el mismo día de la atención, para asegurar su oportuna notificación.** En el Oficio N°1.222, de 30 de marzo de 2020 emitido por SUSESO, "el número 9 abordó la situación de las atenciones médicas ambulatorias, precisando que si el organismo administrador y el trabajador disponen de los medios tecnológicos necesarios, será posible otorgar atenciones médicas en forma remota y en tiempo real, con el debido resguardo de la privacidad y seguridad de la información médica del paciente." "De igual modo se indicó que cuando proceda otorgar al paciente su alta laboral o alta médica, tales indicaciones podrán formalizarse a través de medios alternativos para evitar exponerlo al riesgo de contagio velando, en todo caso, porque tanto él como su empleador sean oportuna y debidamente notificados de su otorgamiento."