NORMA GENERAL TÉCNICA N°237 ESTÁNDARES ASOCIADOS A LAS ACCIONES Y PRESTACIONES DE SALUD A DISTANCIA Y TELEMEDICINA

Ministerio de Salud. “Norma Técnica de Telemedicina”
Primera Edición - 2024

I. PARTICIPANTES EN LA ELABORACIÓN Y REVISIÓN DEL DOCUMENTO

ELABORACIÓN DEL DOCUMENTO

Subsecretaría de Redes Asistenciales	
María José Letelier Ruiz	Departamento de Salud Digital
Eva Guzmán Morales	Departamento de Salud Digital
Pablo Almendras	Departamento de Salud Digital

Subsecretaría de Salud Pública	
Jorge Pacheco Jara	Departamento de Información y Estadísticas en Salud (DEIS)
Pamela Suarez Ojeda	Departamento de Información y Estadísticas en Salud (DEIS)
Patricio Aguilera Vásquez	Departamento de Información y Estadísticas en Salud (DEIS)

Gabinete Ministerial	
Jorge Herrera Reyes	Departamento de Tecnologías de la Información y comunicación (TIC)
María Loreto Rodríguez Guzmán	Departamento de Tecnologías de la Información y comunicación
José Villa Catalán	Departamento de Tecnologías de la Información y comunicación
Lorena Donoso Abarca	División Jurídica

REVISIÓN DEL DOCUMENTO

Gabinete Ministerial	
Yeni Varas Meneses	División de gestión de la red asistencial (DIGERA)
Paulo Villarroel Tapia	División de gestión de la red asistencial (DIGERA)
Anamari Avendaño Arechavala	División de gestión de la red asistencial (DIGERA)
Susana Fuentealba Cofré	División de gestión de la red asistencial (DIGERA)
Nelson Medina Leal	Servicio de Salud Biobío
Cristóbal Sepúlveda Escobedo	Servicio de Salud Metropolitano Central
Ricardo Ahumada Oliva	Servicio de Salud Metropolitano Sur
Catherine Soto Sanhueza	Servicio de Salud Araucanía Sur
Joanna Sandoval Reyna	Servicio de Salud Ñuble
Jenny Obando Latorre	Servicio de Salud Aysen
Viviana Cantín Caro	Servicio de Salud Concepción

CONVOCADOS A REVISIÓN DEL DOCUMENTO

Nombre	Institución que representa
Jaime Ahumada Sandoval	Asociación Chilena de Municipalidades
Jaime Araya Guerrero	Asociación Chilena de Empresas de Tecnología (Chiletec)
Angélica Avendaño Riquelme	Centro Regional de Telemedicina BIO BIO
Jessica Carrasco Ortiz	Asociación Chilena de Municipalidades
Andrés Chacón Bravo	Asociación de Municipalidades de Chile (Amuch)
May Chomalí Garib	Centro Nacional en Sistemas de Información en Salud (CENS)
Camilo Cid García	Fondo Nacional de Salud (FONASA)
Terry de Saint Pierre Guzmán	Asociación Chilena de Empresas de Tecnología de Información (ACTI)
Jean-Jacques Duhart Saurel	Asociación Chilena de Proveedores de la Salud (ProSalud)
Javier Fuenzalida Ríos	Asociación de Clínicas de Chile
César Galindo Vásquez	Health Level Seven Chile (HL7 Chile)
Antonio García Benavente	Instituto de Salud Pública (ISP)
Gabriela Garnham Montes	Asociación de Dispositivos Médicos de Chile (ADIMECH)
Stephen Hartel Urra	Red de Salud Digital de Universidades del Estado (RSDUE)
Martín Kozac Fernández	Asociación Chilena de Empresas de Tecnología de Información (ACTI)
Isabel López Ortega	Red Universitaria Nacional de Telemedicina (RUTE Chile)
Mercedes López Fuentes	Colegio Médico
Maurizio Mattoli Sánchez	Centro Regional de Telemedicina BIO BIO
Francisco Méndez Cáceres	Asociación Chilena de Empresas de Tecnología (Chiletec)
María Macarena Molina Rivas	Red de Salud Digital de Universidades del Estado (RSDUE)
Carmen Monsalve Contreras	Superintendencia de Salud
Tamara Ramírez Vial	Red Universitaria Nacional de Telemedicina (RUTE Chile)

II. CONTENIDO

I. PARTICIPANTES EN LA ELABORACIÓN Y REVISIÓN DEL DOCUMENTO 3

II. CONTENIDO 5

III. ABREVIATURAS 7

IV. PRESENTACIÓN 7

V. INTRODUCCIÓN 8

VI. OBJETIVOS Y ALCANCES 9

A. Objetivo General 9

B. Objetivos específicos 9

C. Alcances 9

VII. MARCO CONCEPTUAL 10

A. La telemedicina en el marco de la estrategia mundial sobre salud digital 2020-2025 de la OMS 10

B. Antecedentes de la telemedicina en Chile 11

C. Términos y definiciones 12

D. Actividades de telemedicina más utilizadas a nivel nacional 14

VIII. MARCO NORMATIVO 15

A. El marco constitucional de la telemedicina en Chile 15

B. Marco legal 16

i. Marco general de la telemedicina 16

ii. Reglamento de atenciones a distancia 18

IX. ESTÁNDARES APLICABLES AL PROCESO DE ATENCIÓN A DISTANCIA Y TELEMEDICINA 21

A. Aspectos sustantivos del otorgamiento de prestaciones a través de telemedicina 21

1. Cumplimiento del deber de información 21

2. Obtención del consentimiento 22

3. Accesibilidad 23

4. Proceso de atención 23

a. Identificación fehaciente de las partes del proceso de atención: (arts. 9 y 11 de la ley N° 20.584; artículos 14 y 16 decreto N°6, 2022, MINSAL) 23

b. Acceso a la información clínica del paciente: (art. 13 ley N° 20.584; arts. 15 y 16 del decreto N° 6 de 2021 de MINSAL; decreto N° 41 de 2012 de Minsal) 24

c. Registro en la ficha clínica: (arts. 12, 14, 31, 37, 39 de la ley N° 20.584; art. 7, 8, 9, 12, 13, 16 del decreto N° 6, de 2021 de MINSAL y decreto 41 de 2012, ambos de Minsal) 24

d. Entrega al paciente del informe y registro de atención (artículos 10 Ley N°20.584, artículo 16 del decreto N° 6, de 2021 de MINSAL) 25

e. Notificación de Enfermedades Transmisibles de Declaración Obligatoria y su Vigilancia. (art. 19 del decreto N° 6, de 2021 de MINSAL; decreto supremo N° 7, de 2019, de MINSAL) 25

5. Supresión o cancelación de datos 25

6. Otras medidas organizativas que debe adoptar el prestador 25

B. Aspectos relativos a las plataformas y sistemas 26

1. Acreditación (artículo 10 bis de la ley Nº 20.584) 26

2. Reglas aplicables al tratamiento de datos personales (artículo 12 de la ley N° 20.584; artículo 16 decreto Nº 6, 2022, MINSAL) 27

a. Privacidad desde el diseño 27

b. Responsabilidad demostrable: (art. 3° ley N° 20.584) 27

c. Protección extendida (artículos 12 y 13 Ley 20.584; 101 del Código Sanitario; artículos 10 al 15 decreto Nº6, 2022, MINSAL) 27

d. Gestión de riesgos de privacidad 27

e. Resguardo de la calidad de datos 28

f. Cumplimiento de los principios de protección de datos personales 28

3. Estándares de seguridad de la información en el otorgamiento de acciones y prestaciones a distancia y telemedicina (Artículo 3 de la ley Nº 20.584; artículos 7, 8 y 9 decreto Nº6, 2022, MINSAL) 29

a. Gobernanza en Seguridad (artículo 3 de la ley Nº 20.584; art. 13 del decreto Nº6, 2022, MINSAL) 30

b. Diseñar, aprobar a implementar políticas y procedimientos de seguridad de la información (art. 13 del decreto Nº6, 2022, MINSAL) 30

c. Implementar políticas de privacidad y tratamiento de datos personales (art. 13 del decreto Nº6, 2022, MINSAL) 31

d. Implementar controles de acceso y trazabilidad de las operaciones realizadas sobre los datos y sistemas 31

e. Sistemas de ficha clínica diseñados para interoperar: (art. 13 de la ley N° 20.584) 31

f. Transmisión segura de la información clínica. (art. 13 de la ley N° 20.584; art. 7 del decreto Nº 6 de diciembre de 2022, MINSAL) 31

g. Plan de gestión de seguridad de la información: (artículos 8 y 9, decreto Nº6 de 2022 de MINSAL) 32

X. SANCIONES Y CUMPLIMIENTO LEGAL 35

XI. GLOSARIO DE SEGURIDAD DE LA INFORMACIÓN 35

XII. VIGENCIA Y ACTUALIZACIÓN 37

XIII. BIBLIOGRAFÍA 38

III. ABREVIATURAS

OMS	Organización mundial de la salud
GES	Garantías Explícitas en Salud
RISS	Redes Integradas de Servicios de Salud
OPS	Organización Panamericana de la Salud
MINSAL	Ministerio de Salud
CMBD	Conjunto Mínimo Básico de Datos
DEIS	Departamento de Estadística e Información de Salud
REM	Resúmenes estadísticos mensuales
TIC	Tecnologías de la Información y Comunicación
ENS	Estrategia Nacional de Salud

IV. PRESENTACIÓN

La ley 21.541, de 03 de marzo de 2023, que modifica la ley N° 20.584, para autorizar a los prestadores de salud a efectuar atenciones mediante telemedicina y su reglamento, aprobado mediante decreto 6 de abril de 2021, de Minsal, publicado en el Diario Oficial el 09 de diciembre de 2022, reglamento sobre acciones vinculadas a la atención de salud realizada a distancia, prevé que MINSAL elaborará una norma técnica para regular distintos aspectos técnicos asociados a la nueva normativa. Recientemente, la ley N° 21.668 de 23 de mayo de 2024, modificó la Ley N° 20.584 con el objeto de establecer la interoperabilidad de las fichas clínicas.

Esta ley consolida legislativamente el Programa Nacional de Telesalud, aprobado por resolución exenta Nº 342, de 9 de marzo del año 2018, del Ministerio de Salud, el cual estableció la Teleasistencia como una estrategia que permite vincular a las personas con la Red de Salud, utilizando las herramientas tecnológicas y de telecomunicación disponibles. En esta misma línea, el decreto supremo Nº 22, del año 2019, del Ministerio de Salud, que aprueba Garantías Explícitas en Salud del Régimen General de Garantías en Salud, en el inciso primero de su artículo 8º, facultó otorgar las prestaciones garantizadas por medio del "[...] uso de las tecnologías de información y comunicación aplicadas en el ámbito de la salud, incluyendo salud digital, tales como las atenciones de telemedicina, teleconsultas, entre otras [...]".

Adicionalmente, el año 2019, se reconoció el código de arancel Fonasa para consultas por telemedicina en la Modalidad de Atención Institucional y, en 2020, antes de la pandemia por Covid-19, se reconocieron códigos de prestaciones por telemedicina en distintas especialidades en la Modalidad Libre Elección.

En este contexto, el Ministerio de Salud ha elaborado esta ''Norma Técnica de Telemedicina'' la cual establece lineamientos y estándares específicos sobre el procedimiento de atención en las prestaciones de salud mediante "telemedicina", "teleasistencia", "teleconsulta", entre otras.

Adicionalmente, establece normas relativas al tratamiento de los datos y los estándares de seguridad, a fin de garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos, que permitan dar continuidad al proceso de atención de salud de las personas.

V. INTRODUCCIÓN

A nivel mundial, el uso de Tecnologías de la Información y Comunicación (TIC) para la salud se ha convertido en un área ampliamente desarrollada que busca responder a las necesidades sanitarias existentes. Ya que estas tecnologías y las aplicaciones a las que dan lugar ofrecen la oportunidad de innovar y rediseñar procesos y modelos de atención sanitaria, aprovechando el potencial que entregan para mitigar las barreras de disponibilidad, aceptabilidad, accesibilidad geográfica, y administrativa entre otras.

En los últimos años, Chile ha implementado importantes proyectos de telemedicina, atención a distancia y telesalud, que han sido impulsados desde el mundo público y privado en conjunto con la academia. También se ha avanzado en tecnologías de inteligencia artificial aplicada a las atenciones de salud y su aplicación ha sido útil en la pesquisa de enfermedades, generando un pre-diagnóstico, que luego es confirmado por un médico especialista, además de utilizarse en el seguimiento remoto de personas con enfermedades crónicas, mediante dispositivos biomédicos de monitoreo.

El Ministerio de Salud ha reconocido los beneficios de la telemedicina, y su contribución en mejorar el acceso, cobertura, oportunidad de la atención y disminución de las listas de espera, dando eficiencia y calidad al Sistema de Salud. En este contexto, el Ministerio impulsó la dictación de la ley N° 21.541, que modificó la ley N° 20.584 para autorizar a los prestadores de salud a efectuar atenciones mediante telemedicina, y del Decreto N° 6, de 2021, del Ministerio de Salud, Reglamento sobre acciones vinculadas a la atención de salud realizada a distancia.

De acuerdo con estas normas, deberá contarse con estándares técnicos y operativos para la utilización de estas tecnologías en la provisión de las acciones y prestaciones de salud por las instituciones del sector público y privado.

VI. OBJETIVOS Y ALCANCES

A. Objetivo General

Establecer los estándares técnicos que permitan dar cumplimiento a lo establecido en la normativa vigente sobre la regulación de las acciones y prestaciones vinculadas a la atención de salud realizadas a distancia, por medio o apoyo de TIC.

B. Objetivos específicos

Establecer estándares asociadas a la atención de salud digital y los sistemas que lo soportan en cumplimiento de lo dispuesto en la ley N° 20.584 de derechos y deberes del paciente, de acuerdo a lo previsto en la ley N° 21.541 y el Decreto N° 6 que regula las acciones vinculadas a la atención de salud realizada a distancia, reglamento de esta última ley. Definir estándares y medidas de seguridad de la información y protección de datos personales destinadas a garantizar la confidencialidad, integridad y disponibilidad de los datos clínicos en el ámbito de las atenciones mediante telemedicina.

C. Alcances

Los lineamientos previstos en esta norma técnica deben ser observadas por todas las partes involucradas en la prestación de servicios de salud a distancia, lo que incluye todos/as los/as prestadores institucionales o individuales -públicos o privados- que realicen acciones necesarias para la promoción, protección, prevención, diagnóstico, tratamiento, recuperación, seguimiento y monitoreo, rehabilitación, cuidados al final de la vida y cualquier otra acción de salud que, por su naturaleza, sea posible de ser realizada mediante la modalidad de "telemedicina", "teleconsulta", "teleasistencia" y otras acciones y prestaciones susceptibles de ser realizadas con apoyo de tecnologías de la información y comunicaciones, además de los proveedores de software y dispositivos de telemedicina, entidades reguladoras, profesionales de la salud y pacientes.

La norma incluye a todos los procesos asistidos por sistemas de información clínica, incluyendo, entre otros:

- Sistemas de agendamiento;
- Sistemas de Información Hospitalaria y Registro Médico Electrónico (HIS-EMR);
- Sistema de Información de Laboratorio (LIS),
- Sistema de Información de Radiología, Sistema de Comunicación y Archivado de Imágenes (RIS- PACS);
- Sistemas de Farmacia;
- Bases de datos de fármacos;
- Sistemas de administración del cuidado del paciente;
- Software de dietas;
- Sistema informatizado de entrada de órdenes médicas (CPOE);
- Sistemas de análisis de grandes volúmenes de datos, siempre que sean utilizados para analizar información obtenida u entregada mediante atenciones médicas digitales;
- Servicios contratados en nube;
- Dispositivos médicos de apoyo al diagnóstico o continuidad del cuidado usados en el marco de las prestaciones de telemedicina.

Esta norma técnica no sustituye los protocolos y lineamientos técnicos asociados a los aspectos sustantivos de las acciones o prestaciones de salud, por lo que cada una de ellas se regirá por los lineamientos que defina la autoridad para cada caso.

VII. MARCO CONCEPTUAL

A. La telemedicina en el marco de la estrategia mundial sobre salud digital 2020-2025 de la OMS

La 73ª Asamblea Mundial de la Salud, mediante su acuerdo WHA73 refrendó la "Estrategia Mundial sobre Salud Digital 2020-2025" plantea 8 principios para la transformación digital del sector Salud, que orientan la estrategia mundial hacia una adopción adecuada y sostenible de las tecnologías de salud digital en el contexto de las estrategias nacionales relativas al sector sanitario y a la salud, a los que nos referiremos a continuación[1]:

1. Conectividad universal del sector salud para 2030 con ancho de banda suficiente para el abordaje de las necesidades y desafíos del sector.
2. Bienes públicos digitales para fortalecer la salud y el bienestar de la población mundial debe incluir software de código abierto, normas, algoritmos, datos, aplicaciones y contenidos diseñados con la arquitectura y el licenciamiento adecuados.
3. Salud Digital Inclusiva que considere acceso apropiado, habilidades digitales y aspectos de usabilidad y navegabilidad en el desarrollo de soluciones tecnológicas, sin dejar de respetar la autonomía de las personas y poblaciones que decidan no utilizar los servicios digitales.
4. Interoperabilidad, apertura y sostenibilidad de los sistemas, que proporcionen acceso oportuno y abierto a datos correctamente desagregados, integración de los sistemas nacionales y locales, salud digital y TIC.
5. Protección de los derechos humanos: la dignidad humana, en su dimensión individual y social, debe ser uno de los valores fundamentales de este proceso, como también lo es el medio ambiente donde se desarrolla la vida. Para ser justo y equitativo, el marco normativo debe estar desprovisto de todo sesgo geográfico, educativo, cultural, político, religioso o de género.
6. Cooperación Mundial en Inteligencia Artificial que comprenda la dimensión individual y social en una realidad globalizada e interconectada y promueva los enfoques de equidad, género y diversidad cultural con algoritmos seguros, confiables y abiertos.
7. Seguridad de la información: Los sistemas deben implantarse respetando los derechos relativos a la salud, a fin de generar una "cultura de manejo de datos seguros y confiables", entendida como el equilibrio entre la necesidad de acceder a los datos y la protección de datos sensibles de salud, así como pautas y normas internacionales de seguridad para los sistemas de información centrados en el paciente.
8. Arquitectura de la salud pública enmarcada en la agenda digital del gobierno de manera transversal, para articular las distintas vertientes de gobernanza y optimizar la planificación estratégica y la gestión de los recursos. Debe basarse en el aprovechamiento de normas y procedimientos a favor de múltiples áreas, no solo de la esfera de la salud, sino en las demás áreas, rales como la educación, el trabajo y en todos los sectores de una sociedad moderna.

[1] OPS-OMS. "8 Principios para la transformación digital del sector salud". Disponible en línea en https://www.paho.org/es/8-principios-para-transformacion-digital-sector-salud. 2021

Con el fin orientar y coordinar la transformación digital la Organización Mundial de la Salud define los siguientes objetivos estratégicos asociados a la salud digital[2]:

Objetivos Estratégicos	Resultados Esperados
Promover la colaboración en el plano mundial y fomentar la transferencia de conocimientos de salud digital.	Un ecosistema de salud digital cada vez más adecuado y sostenible.
Impulsar la ejecución de estrategias nacionales de salud digital.	Sistemas y servicios de salud eficaces y eficientes en función del costo.
Fortalecer la gobernanza en pro de la salud digital en los planos mundial, regional y nacional.	Digitalización acelerada del sector de la salud y el bienestar.
Propugnar sistemas de salud centrados en las personas facilitados por medio de la salud digital.	Poblaciones más sanas.

B. Antecedentes de la telemedicina en Chile

La Reforma de Salud del año 2004 (Ley de Autoridad Sanitaria N° 19.937), estableció como parte de la función rectora del Ministerio de Salud (MINSAL), la definición de objetivos sanitarios y en torno a ellos, y el desarrollo de procesos de planificación sanitaria. La Estrategia Nacional de Salud 2021-2030, incorporó como un objetivo de impacto el desarrollo de un modelo de atención de salud digital sostenible, que aporte al acceso, la atención oportuna y la información a los pacientes en sus contextos territoriales/culturales, de manera articulada, coordinada y que complemente al modelo de atención de salud presencial vigente, y previó dentro de los resultados esperados del mencionado objetivo de impacto, el fortalecimiento del desarrollo de capital humano sectorial y la alfabetización digital de los usuarios y la comunidad en salud digital; el fortalecimiento de la inversión y el desarrollo de las tecnologías para la salud digital y el adecuado financiamiento de la inversión, mantención y operación; la definición de la gobernanza y establecimiento de un marco regulatorio claro y eficiente en el modelo de salud digital y de los sistemas de información del intersector.

Hoy en día nos enfrentamos a un nuevo escenario por el aumento de la movilidad de la población, los cambios a nivel socioeconómico y demográfico y de las condicionantes de salud, como el envejecimiento o las enfermedades crónicas no transmisibles, todo lo cual plantea la necesidad de evaluar e incorporar nuevas alternativas que aborden estos desafíos, contribuyendo a dar respuesta a las brechas de inequidad existentes.

En el año 2018, la Asamblea Mundial de la Salud reconoció el valor de las tecnologías digitales para contribuir al avance de la Cobertura Universal de Salud, instando a los estados miembros a evaluar su uso.[3] Nuestro país asumió el reto de mejorar los indicadores y condiciones de salud de la población, identificando las falencias que afectan la salud de las personas, como el déficit de especialistas, de infraestructura y gestión, entre otras, y proponiendo avanzar en estas áreas a fin de mejorar en el acceso y oportunidad a servicios de salud de calidad.

La incorporación y utilización de la telemedicina en la provisión de servicios de salud ha permitido, entre otros beneficios, optimizar el recurso humano especializado, complementando acciones y soluciones que permiten una mejora sustancial en el acceso a especialistas para aquellos territorios alejados o que presentan problemas de oferta. Así, la telemedicina ha permitido implementar una estrategia que permite suministrar servicios de salud integrales, destinados a mantener el bienestar general de las personas, mejorar su estado de salud y la continuidad de sus cuidados.

[2] OMS, Datos e innovación: proyecto de estrategia mundial sobre salud digital. Informe del Director General, aprobado en la 146ª. Reunión, EB146/26, 23 de diciembre de 2019.

[3] Resolución WHA 71/A del 21 de mayo 2018.

En este sentido, la telemedicina es mucho más que la mera transmisión de información y comunicación entre pacientes y equipos de salud o la utilización de las tecnologías en la provisión de servicios de salud. Hoy en día se le reconoce como una modalidad de atención, que a medida que se inserta y desarrolla como parte de un proceso clínico dentro del marco de las Redes Integradas de Servicios de Salud, se ha consolidado como una estrategia efectiva, no siendo un fin en sí misma, sino que parte, apoyo y complemento de las atenciones presenciales, que facilita los procesos asistenciales, suministrando además información sanitaria valiosa para la gestión y la toma de decisiones.

En relación con el desarrollo de la salud digital y la telemedicina, cabe tener presente que el Ministerio de Salud, creó en 2007 el Departamento de Asistencia Remota en Salud; en 2012, implementó Teleradiología y Teleasistencia a través de dispositivos móviles y, en 2017, creó la "Red de Referencia de Telemedicina en Ataque Cerebro Vascular" en el Servicio de Salud Metropolitano Sur. En 2018 dispuso el "Programa Nacional de Telesalud 2018[4]", el cual tenía por objetivo generar lineamientos técnicos y tecnológicos para desarrollar la Teleeducación, Telemedicina y Teleasistencia en los Servicios de Salud y en 2019, se creó el Departamento de Salud Digital, con el fin de facilitar la provisión de servicios de salud a distancia en las redes asistenciales.

Adicionalmente, el año 2019, se reconoció el código de arancel Fonasa para consultas por telemedicina en la Modalidad de Atención Institucional y, en 2020, antes de la pandemia por Covid-19, se reconocieron códigos de prestaciones por telemedicina en distintas especialidades en la Modalidad Libre Elección.

Con ocasión de la pandemia por coronavirus, el Ministerio de Salud autorizó el uso de códigos para las atenciones remotas durante el período de vigencia de la Alerta Sanitaria. Una de las últimas normativas en periodo de alerta sanitaria fue la Ley N° 21.267, que establecía medidas para facilitar la adquisición de remedios en el contexto de una alerta sanitaria por una epidemia o pandemia, la que sólo se mantuvo vigente durante la alerta sanitaria Covil-19.

C. Términos y definiciones

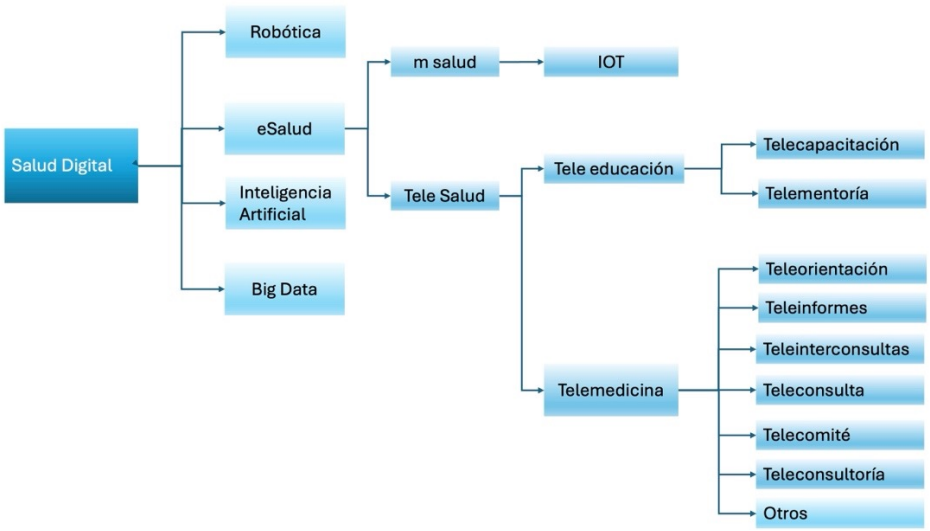
El marco conceptual propuesto se organiza con una visión de proceso de las acciones y prestaciones otorgadas en modalidad telemedicina, refiriéndose a los sujetos de la intervención, temporalidad, herramientas necesarias, registros asociados y contexto de la misma prestación, lo que facilita su operacionalización en procesos y subprocesos claves tales como la implementación, programación, agendamiento, reportería, monitoreo y evaluación. Para estos efectos utilizaremos lo previsto en el decreto N°6, de 2021 y en la ley 20.584 modificada por la ley N° 21.541, además de los instrumentos propuestos por organismos internacionales tales como la OMS-OPS:

- **Acciones o prestaciones de salud remota o a distancia apoyadas en TIC:** comprende las acciones necesarias para la promoción, protección, prevención, diagnóstico, tratamiento, recuperación, seguimiento y monitoreo de la condición de la persona, rehabilitación, cuidados al final de la vida y, en general, todo tipo de acción de salud que, por su naturaleza, sea posible de ser realizada a distancia que se realice a través o con el apoyo de TIC.
- **Acciones o prestaciones de salud con apoyo de sistemas automatizados:** incluye todas las acciones o prestaciones de salud otorgadas a través de herramientas tecnológicas tales como aplicaciones, robótica, inteligencia artificial, Internet de las Cosas (IoT), entre otras, en la medida que la naturaleza de las acciones o prestaciones lo admitan y que se garantice la calidad de

[4] Ministerio de Salud, Subsecretaria de Redes Asistenciales. Programa Nacional de Telesalud en el contexto de redes integradas de los Servicios de Salud.

la atención, la autonomía de la voluntad del paciente, la seguridad y la confidencialidad de los datos de las personas.

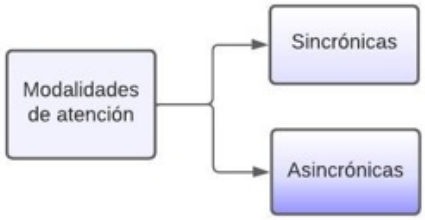
- **Herramientas tecnológicas al servicio de las acciones y prestaciones de salud a distancia:** los programas computacionales y los dispositivos a que se refiere el artículo 4 del decreto N° 6, de 2021 de Minsal, así como las aplicaciones y los soportes, sistemas o plataformas a las que se refiere el art. 10 bis de la ley N° 20.584, a través de los cuales se puedan realizar acciones y prestaciones vinculadas con la salud a distancia, o que sirvan de apoyo a éstas.
- **Salud Digital:** la OMS define salud digital como el campo del conocimiento y la práctica relacionado con el desarrollo y la utilización de las tecnologías digitales para mejorar la salud. Amplía el concepto de cibersalud o e-Salud para incluir a consumidores digitales, junto a una gama más amplia de dispositivos inteligentes y equipos conectados. También abarca otros usos de las tecnologías digitales como el internet de las cosas (Internet of Things, IoT), la inteligencia artificial, Big Data y la robótica, tal y como se reconoce en el decreto N° 6 de 2021, de MINSAL.



- **Telesalud:** corresponde a una estrategia basada en el Modelo de Atención Integral de Salud Familiar y Comunitaria, en el contexto de las Redes Integradas de Servicios de Salud (RISS), y que mediante el uso de las tecnologías de información y comunicaciones, facilita la provisión de servicios a distancia desde el ámbito de la promoción, prevención, diagnóstico, tratamiento, rehabilitación y cuidados paliativos, centrado en la persona en su contexto sociocultural y a lo largo de su curso de vida, con el propósito de mantener un óptimo estado de salud y la continuidad de cuidados de la población, mejorando así la equidad en el acceso, el ejercicio de derechos, la oportunidad y la calidad de la atención.
- **Telemedicina:** corresponde a la provisión de servicios de salud a distancia mediante el uso de las tecnologías de la información y comunicación y permite realizar diagnósticos, tratamiento, promoción, prevención, rehabilitación y cuidados de fin de la vida. Es realizada por profesionales de la salud, permitiendo intercambiar datos con el propósito de facilitar el acceso y oportunidad, asegurando la calidad y continuidad de la atención.

De acuerdo con la temporalidad, las actividades de telemedicina que impliquen una interacción entre las partes se pueden diferenciar en:

- **Sincrónica:** Corresponde a la interacción en "tiempo real y en vivo" que permite las comunicaciones entre uno o más integrantes del equipo de salud entre sí, o entre el paciente y el equipo de salud.
- **Asincrónica:** Corresponde a la interacción "diferida", que permite el almacenamiento y transmisión de datos e imágenes, los que son enviados a un profesional de la salud, junto con antecedentes clínicos del paciente, para que este emita un diagnóstico y tratamiento.



D. Actividades de telemedicina más utilizadas a nivel nacional

Teleconsulta: Se refiere a la actividad de interacción que ocurre entre un profesional de la salud y un paciente, con el objetivo de otorgar una atención con fines diagnósticos o terapéuticos a través de tecnologías de la información y comunicaciones (ej. videollamada). Durante la teleconsulta podrían participar otros miembros del equipo de salud que se encuentran físicamente al lado de la persona atendida, acompañando o facilitando la atención. Esta prestación puede realizarse de manera sincrónica o asincrónica o diferida.

- **Teleinterconsulta:** corresponde a una prestación de salud a distancia, que puede ser sincrónica o asincrónica, en la que profesionales de la salud intercambian información sobre un caso clínico utilizando tecnologías de la información y comunicación con fines diagnósticos, terapéuticos y de seguimiento.
- **Teleinforme:** Corresponde al informe generado a la distancia por un profesional de la salud y/o especialista en base a los datos obtenidos a través de un examen o procedimiento diagnóstico que se ha realizado en otro lugar. También incluye informes realizados mediante Inteligencia Artificial.
- **Teleconsultoría:** Corresponde al intercambio de información, opiniones y sugerencias sobre casos clínicos entre miembros del equipo de salud a la distancia, realizadas a través de tecnologías de la información y telecomunicaciones en modalidad sincrónica.

  El objetivo principal de la teleconsultoría es la t**ransmisión de conocimientos entre los equipos de salud.** Puede ser utilizada para que un grupo de profesionales de salud comparta definiciones o sugerencias con otro grupo de profesionales en torno a un problema común.
- **Telemonitoreo:** consiste en recopilar, registrar, almacenar y procesar datos de parámetros fisiológicos, mediante dispositivos que permitan transmitir electrónicamente información que requiera de monitoreo. Los profesionales de la salud supervisan y evalúan estos de forma remota y, cuando es necesario, intervienen realizando acciones de salud. (ej.: monitoreo de pacientes crónicos).

- **Telecomité:** Corresponde a la interacción sincrónica o asincrónica entre un equipo multi y/o interdisciplinar mediante el uso de tecnologías de información y comunicación para evaluar casos clínicos y tomar decisiones consensuadas relacionadas con el diagnóstico, tratamiento, y continuidad del cuidado del sujeto de intervención. (ej.: Telecomité Oncológico)
- **Telerehabilitación:** Consiste en la provisión de servicios de rehabilitación mediante el uso de TIC, entregados por un profesional o equipo de salud a un paciente y/o grupo de pacientes. Esta modalidad puede considerar una amplia gama de intervenciones clínicas asociadas a la rehabilitación.
- **Teletriage:** Actividad o proceso no agendado dirigido a determinar la prioridad de la atención que requieren los pacientes en función de la gravedad de su condición de salud o afección, realizado por miembros del equipo de salud a través del uso de tecnologías y de la información y comunicación.

VIII. MARCO NORMATIVO

A. El marco constitucional de la telemedicina en Chile

El texto constitucional vigente, en el artículo 19 N° 1, modificado por la ley N° 21.383 prevé que *"el desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella"*. De ello desprendemos que las ciencias médicas y con ello la telemedicina debe cumplir con los siguientes imperativos:

i. **Bienestar de la persona:** Las acciones y prestaciones de salud en general y las de telemedicina en particular deben tender al bienestar de la persona y en la evaluación de riesgos debe ser mayor el beneficio esperado que los eventuales efectos adversos.

ii. **Primacía de la persona:** Se trata de anteponer a la persona y su bienestar al deseo de hacer avanzar la ciencia y la tecnología. En el ámbito de la salud digital se traduce en la necesidad de que la investigación asociada a las tecnologías de salud digital anteponga el bienestar de los usuarios del sistema por sobre el interés en el desarrollo tecnológico.

iii. **Licitud:** Las acciones y prestaciones de salud, cualquiera sea la tecnología que emplee, debe cumplir la normativa vigente en cada momento.

A continuación, el artículo 19 N° 4 de la Constitución Política de la República reconoce *"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"*. Esta norma a continuación establece que *"El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley"*. De este artículo desprendemos los siguientes principios rectores aplicables al tratamiento de datos personales y los sistemas empleados en el marco de las acciones y prestaciones de telemedicina:

i. **Finalidad:** El tratamiento de la información de la persona debe ser compatible con las necesidades de garantizar las acciones de promoción, protección, recuperación de la salud y demás cuidados que requiera la persona en todas las etapas de su vida.

ii. **Licitud:** Además de lo señalado en la letra a.- de este acápite, en este caso se agrega el cumplimiento de las normas y principios del tratamiento de datos personales, previstos en

la ley N° 19.628, en la ley de firmas y documentos electrónicos N° 19.799 y sus normas reglamentarias. Tratándose de las instituciones públicas y privadas en convenio, las normas de protección de datos deberán concordarse con las de la ley N°20.285, de transparencia y acceso a la información pública.

iii. **Calidad de datos:** La información que conste en la ficha clínica debe ser completa, auténtica y verídica, de forma tal que el personal de la salud que conforme a la ley pueda tener acceso a ella pueda conocer en cada momento la información necesaria para la realización y otorgamiento de las acciones y prestaciones de salud que corresponda.

iv. **Seguridad:** La seguridad en este ámbito dice relación con la adopción de las medidas técnicas y administrativas que permitan garantizar la autenticidad, disponibilidad y confidencialidad de la información de salud de los pacientes. Son tales, la definición de perfiles con atributos diferenciados de acceso, lectura o escritura de información en los documentos asociados a las prestaciones de salud, tales como la ficha clínica, la receta, órdenes y resultados de exámenes. También entran en esta categoría la definición de canales seguros de comunicación y transferencia de datos entre prestadores, y la segregación de datos, entre otras.

Finalmente, el art. 19 N° 9 de la Constitución Política de la República prevé que *"El Estado protege el libre e igualitario acceso a las acciones de promoción, protección y recuperación de la salud y de rehabilitación del individuo"*. A lo anterior, la doctrina suma los cuidados al fin de la vida, siendo el deber del Estado de garantizar el acceso oportuno a dichas acciones y prestaciones. De esta norma emanan los siguientes principios que rigen respecto de todas las modalidades de atención:

i. **Libertad-Autonomía del paciente:** La persona tiene derecho a ser informada y consentir, ya sea personalmente o a través de la persona bajo cuyo cuidado se encuentre, en las acciones y prestaciones de salud que se le otorguen.

ii. **Igualdad:** El acceso igualitario en el acceso a las acciones de promoción, protección y recuperación de la salud. En Chile, este imperativo se ha llevado adelante a través de leyes de garantía de calidad e igualdad en el acceso a las acciones y prestaciones de salud, tales como la ley N° 19.966, que establece las prestaciones de carácter promocional, preventivo, curativo, de rehabilitación y paliativo, y los programas que el Fondo Nacional de Salud deberá cubrir a sus respectivos beneficiarios, y la ley N° 20.850, que crea un sistema de protección financiera para diagnósticos y tratamiento de alto costo y rinde homenaje póstumo a don Luis Ricarte Soto Gallegos.

iii. **Supervisión y Coordinación:** Corresponde al Estado el deber de garantizar la ejecución de las acciones y prestaciones de salud ya sea en el sistema público o privado.

B. Marco legal

i. Marco general de la telemedicina

El artículo 4 N° 2 del DFL N° 1, de 2005 del Ministerio de Salud, dispone que le corresponde al Ministerio de Salud, "2.- Dictar normas generales sobre materias técnicas, administrativas y financieras a las que deberán ceñirse los organismos y entidades del Sistema, para ejecutar actividades de prevención, promoción, fomento, protección y recuperación de la salud y de rehabilitación de las personas enfermas".

La ley 21.541, modificó la ley N°20.584 de derechos y deberes de los pacientes para los efectos de reconocer que existen distintas modalidades de atención, además de las realizada de manera

presencial, tales como las atenciones "a distancia", o las de "salud digital", que a lo largo del tiempo se la ha denominado de distintas maneras, tales como "telesalud", o "telemedicina".

Esta ley autoriza a los prestadores para *"otorgar acciones, atenciones y procedimientos de salud digital destinados a la prevención, promoción, protección, recuperación y rehabilitación de las personas, manteniendo registros de estas prestaciones en los mismos términos que una atención presencial"*. A continuación, la norma señala que las prestaciones de telemedicina deberán sujetarse a las disposiciones reglamentarias vigentes y las que al efecto dicte el Ministerio de Salud, *"las que tendrán por objeto resguardar que las prestaciones de salud digital se ejecuten en condiciones de seguridad, con respeto a los derechos en salud de las personas y regular la implementación y desarrollo de acciones vinculadas a la atención de salud realizadas a distancia, por medio o con apoyo de tecnologías de la información y comunicaciones"*.

Conforme al mandato legal, el Ministerio de Salud debe dictar las disposiciones reglamentarias y normas técnicas que permita asegurar los siguientes ejes normativos:

1. Seguridad y confidencialidad en el otorgamiento de acciones y prestaciones de salud digital;
2. Garantizar los derechos en salud de las personas, entre los que se cuentan la protección de la vida privada y la honra de la persona (art. 5 letra c, de la ley N°20.584), además de los datos personales de los usuarios del sistema de salud;
3. Regular la implementación y desarrollo de acciones vinculadas a la atención de salud realizadas a distancia. En este ámbito cobran relevancia las siguientes materias:
    i. Los requisitos y procedimientos aplicables a la autorización sanitaria de los prestadores institucionales que otorguen prestaciones de salud digital, y de los espacios asistenciales destinados a ello; al ejercicio de las acciones de telemedicina respecto de los prestadores individuales de salud; y a las medidas de registro, publicidad, calidad, seguridad y de fiscalización que podrán ser tomadas para asegurar el cumplimiento de lo dispuesto en la ley 20.584 (art. 8 bis ley N° 20.584).
    ii. Las plataformas tecnológicas empleadas en las acciones y prestaciones de salud digital, y las que almacenan y tratan datos personales (art. 10 bis ley N° 20.584), y los sistemas de gestión de fichas clínicas (art. 13 ley N° 20.584) deben acreditar el cumplimiento de las normas y estándares técnicos que a su respecto establezca el Ministerio de Salud.

En otro ámbito, la Ley N° 19.966, que establece un régimen de garantías en salud (GES), y el Decreto N° 22/2022 de MINSAL, que aprueba garantías explícitas en Salud del Régimen General de Garantías en Salud, define en su artículo 3° las prestaciones o grupos de prestaciones de salud en los siguientes términos: *"Acciones de salud, tecnologías o dispositivos médicos, tales como consultas médicas, exámenes y procedimientos; medicamentos; artículos farmacéuticos y de laboratorio; material quirúrgico, instrumental y demás elementos o insumos que se requieran para el diagnóstico de un problema de salud y su tratamiento, seguimiento y rehabilitación"*.

El artículo 8 de la mencionada ley prevé que las prestaciones señaladas en el artículo 3° se otorgarán exclusivamente a través de la red de prestadores de FONASA y de las ISAPRE según corresponda, pudiendo hacer uso de las tecnologías de información y comunicación aplicadas en el ámbito de la salud, incluyendo salud digital, tales como las atenciones de telemedicina, teleconsulta y otros usos de salud digital.

ii. Reglamento de atenciones a distancia

La ley N°21.541 reenvía al ámbito reglamentario o de normas técnicas las siguientes materias:

1. inc. 3 art. 3 ley 20.584, Reglamento de Atenciones de Salud de telemedicina, ámbito cubierto por el dto. N°6, de 2021 del Ministerio de Salud que analizaremos a continuación.
2. Art. 8 bis. Ley 20.584, Reglamento de Autorización sanitaria prestadores institucionales de salud digital, materia abordada en el Decreto Supremo N° 15 de 2007, del Ministerio de Salud.
3. Art. 10 bis ley 20.584, Reglamento de acreditación de plataformas tecnológicas de telemedicina, materia que deberá abordarse de manera conjunta con la implementación de los reglamentos y normas técnicas asociados a la ley N° 21.668 de interoperabilidad de fichas clínicas y en base a los estándares tecnológicos previstos en el Decreto N° 6.
4. Art. 13 ley 20.584, Reglamento conjunto con Hacienda: Certificación de estándares técnicos y administrativos de sistemas de ficha clínica, materia que deberá abordarse de manera conjunta con la implementación de los reglamentos y normas técnicas asociados a la ley N° 21.668 de interoperabilidad de fichas clínicas y en base a los estándares tecnológicos previstos en el Decreto N° 6.

Conforme a lo anterior, en 2021 se aprobó el decreto N°6 de 2021, el cual se presentó a la Contraloría General de la República para su aprobación, mientras se discutía en el parlamento la reforma legislativa, concluyendo su tramitación antes de la promulgación de la ley, impulsado por las necesidades sanitarias suscitadas por la gestión de la pandemia por COVID-19.

Sin perjuicio de su aprobación temprana, este decreto es el que regula varias de las materias que la ley N° 21.541 reenvía a Reglamento, por lo que ya se encuentra satisfecho el imperativo legal en dichos ámbitos.

En cuanto a su ámbito de aplicación, este reglamento se aplica **a todos los prestadores referidos en el artículo 3 de la ley Nº 20.584 y en el artículo 3º del decreto supremo Nº 38, de 2012, del Ministerio de Salud,** sin perjuicio de que el prestador individual que interviene en la prestación se encuentre fuera del Territorio de la República, en la medida que el prestador institucional, por medio o a través del cual se presten las acciones o prestaciones de salud se encuentre domiciliado en Chile.

En todo caso, tanto la ley como el decreto excluyen de su ámbito de aplicación los portales que contengan exclusivamente información de salud, los servicios de soporte a la custodia y gestión de historias clínicas, los sistemas de apoyo a la emisión de licencias médicas y recetas electrónicas, así como los sistemas digitales auxiliares para prestaciones de salud, salvo en lo expresamente establecido, que dice relación con el cumplimiento de los estándares de seguridad y protección de datos personales[5].

[5] En relación con la regulación de la receta electrónica, el artículo 101 del Código Sanitario prevé que "La receta profesional deberá ser extendida en documento gráfico o electrónico cumpliendo con los requisitos y resguardos que determine la reglamentación pertinente y será entregada a la persona que la requirió o a un tercero cuando aquella lo autorice. El reglamento establecerá al menos los elementos técnicos que impidan o dificulten la falsificación o la sustitución de la receta, tales como el uso de formularios impresos y foliados, código de barras u otros. Si es manuscrita deberá extenderse con letra imprenta legible. En caso alguno la utilización de receta electrónica podrá impedir que el paciente pueda utilizar este instrumento en el establecimiento farmacéutico que libremente prefiera, pudiendo siempre exigir la receta en documento gráfico".

En el contexto de la gestión de la pandemia, antes de la dictación de la ley N°21.541, la ley Nº 21.267, de 2020, previó que "En caso de decretarse una alerta sanitaria con ocasión de una epidemia o pandemia y durante la vigencia de ésta, los productos farmacéuticos podrán ser expendidos por cualquier establecimiento autorizado para ello, mostrando una copia de la receta médica que los prescriba, ya sea en formato físico o digital, en cualquiera de sus formas", extendiendo la vigencia de las recetas respectivas hasta seis meses después del término de la emergencia.

Esta ley modificó el artículo 101 del Código Sanitario en el sentido que la receta electrónica deberá constar en un documento electrónico suscrito por parte del facultativo autorizado en la ley según lo dispuesto en el reglamento.

En este mismo ámbito, se dictó la resolución exenta N° 1143 de 2023, del Ministerio de Salud, que aprueba el sistema de validación de recetas gráficas y establece lineamientos para la prescripción y dispensación de las recetas gráficas y digitalizadas.

El Decreto regula las siguientes materias atingentes a esta norma técnica, a saber:

1. Estándares Tecnológicos que resguarden la calidad del proceso de atención y la protección de los derechos del paciente: Los prestadores que implementen atención remota deben garantizar:

i. **La identificación inequívoca** tanto de los pacientes como de los profesionales y técnicos de la salud intervinientes.

ii. **La neutralidad tecnológica,** en el sentido que esté diseñada e implementada para interoperar desde el punto de vista semántico y sintáctico, tanto a nivel de datos, sistemas y redes de comunicaciones.

iii. **La transmisión segura de datos e información clínica** necesaria para el otorgamiento de la prestación, utilizando mecanismos fiables y formatos reutilizables que integren reglas de protección de los datos personales, la reserva de la ficha clínica, la ética biomédica, y los derechos y deberes de los pacientes.

iv. **La trazabilidad y registro** de las acciones realizadas con apoyo de TIC.

2. Protección de la privacidad del paciente: Programas computacionales, plataformas y sistemas informáticos, que resguarden la privacidad del paciente y dar estricto cumplimiento a los estándares técnicos que el/la ministro/a de Salud establezca a través de resolución. En este ámbito, se deben cumplir, al menos, las siguientes condiciones:

i. **Disponer de procedimientos específicos de aseguramiento de la confidencialidad,** según la acción o prestación otorgada. A estos efectos los prestadores podrán elaborar sus propios procedimientos o adoptar aquellos que proponga el Ministerio de Salud **mediante norma técnica.** A vía ejemplar, si el paciente concurre a la atención presencial o a distancia mediante telemedicina, asistido por un acompañante, éste debe ser informado de que le asiste el deber de secreto.

ii. **Contar con planes de gestión de riesgos de privacidad,** que le permitan minimizar los riesgos asociados a accesos o divulgación indebida, o una alteración o modificación de los datos personales relativos a los pacientes.

iii. **Utilizar sistemas que cuenten con mecanismos de gestión de los perfiles profesionales** en términos tales que se garantice que cada uno de ellos, dentro del ámbito de sus competencias, tenga acceso eficaz y oportuno a la información que requieren para cumplir su función dentro del proceso de atención al paciente, pero a su vez se resguarde la información de accesos indebidos.

3. Cumplir las obligaciones de seguridad de la información:

i. **Mantener respaldos seguros y funcionales de la información** y contar con las medidas técnicas y organizativas que permitan el restablecimiento de los sistemas de información clínica a fin de garantizar la continuidad de la atención de los pacientes.

ii. **Mantener planes de gestión de riesgos sobre seguridad y confidencialidad de los documentos electrónicos,** en los términos previstos en la ley 19.799 y su normativa reglamentaria, de manera que se permita asegurar la continuidad de los servicios y la integridad, confidencialidad, y disponibilidad de la información.

iii. **Gestión de incidentes:** Adoptar, de forma inmediata, las medidas necesarias para minimizar los efectos nocivos que se hubieren generado con ocasión del incidente, documentar y adoptar las medidas preventivas que permitan mitigar los riesgos de que se produzcan eventos futuros de similar naturaleza.

Dentro de las obligaciones que emanan de este imperativo destacamos la de Registrar incidentes de seguridad de la información y notificarlos al Comité de Seguridad de la Información (CSI) del Ministerio de Salud, del nivel central, respecto de todos los incidentes de seguridad de la información que puedan afectar a los sistemas o a la información que es objeto de tratamiento, dentro de las 72 horas siguientes al momento en que éste haya sido detectado.

4. Resguardo a los Derechos de los Pacientes:

i. **Adoptar medidas de accesibilidad:** Asistencia a personas que no dominen suficientemente las TIC, o que tengan otra condición que le impida hacer uso adecuado de ellas, dejando constancia del consentimiento del paciente y la circunstancia del acompañamiento en la ficha clínica.

ii. **Acceso a la ficha clínica y portabilidad:** Los sistemas deben estar diseñados para permitir que todos los profesionales y técnicos que, dentro de la atención a distancia que realicen acciones de promoción, protección, recuperación de la salud, rehabilitación de la persona y cuidado de fin de vida del paciente pueda acceder a los datos personales contenidos en la ficha clínica, que sean necesarios para la ejecución de las acciones para las cuales se encuentran habilitados por la normativa que les rija, con independencia del prestador institucional al alero del cual realicen las acciones y prestaciones.

iii. **Cumplimiento del deber de información:** Además del deber general de información que prevé la ley N° 20.584, se debe entregar la siguiente información a la persona y/o a su acompañante, en lenguaje comprensible de acuerdo con las necesidades del paciente. Al respecto, este deber conlleva obligaciones tanto en el ámbito técnico y organizativo, y otras asociadas a la modalidad de atención, como se analiza a continuación:

   a. **Información sobre los términos y condiciones de la prestación de los servicios de apoyo a la prestación:** Detalle de las reglas y procedimientos de la prestación de los servicios por medio de los cuales se realiza o se apoya su atención, en caso de que cuenten con páginas web, o servicios vía aplicaciones.

   b. **Políticas de privacidad de los datos:** detalle qué tipo de datos personales serán objeto de tratamiento, la finalidad para la cual serán utilizados, los terceros a los que podrían comunicarse los datos, el tiempo de retención, y una cuenta a través de la cual se puedan ejercer los derechos de acceso, rectificación, y portabilidad de los datos.

   c. **Documentos de seguridad de la información:** Detalle de las reglas de gestión de perfiles, claves de acceso y un contacto al cual comunicar eventuales incidentes de seguridad a que pudieren verse expuestos los sistemas y servicios tecnológicos empleados en la provisión de las acciones y prestaciones de salud a distancia por TIC.

   d. **Condiciones técnicas requeridas:** Equipamiento, conectividad, aplicaciones, sistemas de autenticación con los que debe contar el paciente el día de la atención para que ésta pueda llevarse a cabo correctamente.

   e. **Información sobre la grabación de la atención:** Si el servicio considera la grabación de la atención y, en caso de contar con ello, el tiempo por el cual se conservarán los registros y posibles comunicaciones a terceros.

f. **Información suficiente sobre la prestación:** Denominación y descripción del tipo de acción o prestación de que se trate, explicando los beneficios y riesgos sanitarios asociados a la realización de la prestación en modalidad a distancia, con apoyo de TIC.

g. **Identificación y autenticación del prestador:** los sistemas y aplicaciones utilizados, deben mostrar, desde su inicio y durante toda la atención, el nombre completo y apellidos del prestador individual y su función; el prestador institucional al que pertenece, si corresponde; y el correo electrónico o teléfono al que le podrán dirigir comunicaciones. Esta información debe desplegarse en letra legible, en idioma castellano y de fácil comprensión. Sin perjuicio de lo anterior, la información podrá entregarse, además, en otro idioma si este fuera inteligible por el paciente o por la persona bajo cuyo cuidado se encuentre, en caso de que corresponda.

iv. **Consentimiento informado en la modalidad de atención:** Además de las reglas generales del consentimiento previstas en la ley N°20.584, el paciente o la persona bajo cuyo cuidado se encuentre si éste no está en condiciones de otorgarlo, deberá consentir en la modalidad de atención, para ello esta norma técnica prevé la forma como se debe cumplir con esta obligación.

IX. ESTÁNDARES APLICABLES AL PROCESO DE ATENCIÓN A DISTANCIA Y TELEMEDICINA

A. Aspectos sustantivos del otorgamiento de prestaciones a través de telemedicina

1. Cumplimiento del deber de información

Tratándose del otorgamiento de acciones o prestaciones a distancia y telemedicina, los prestadores deberán informar al paciente o, en su caso, a la persona que le dé asistencia, en lenguaje comprensible, acorde al estado de salud del paciente y sus características socio culturales, los contenidos que señala el art. 13 del decreto N° 6, de 2021 de Minsal, a saber:

i. **Denominación y descripción del tipo de acción o prestación de que se trate:** explicando los beneficios y riesgos sanitarios asociados a la realización de la prestación en modalidad a distancia, con apoyo de TIC.

ii. **Los sistemas y plataformas que se usarán en el otorgamiento de acción o prestación. Las condiciones técnicas con que debe contar el paciente:** Se debe informar las condiciones de conectividad con que debe contar el paciente el día de la atención para que ésta pueda llevarse a cabo correctamente.

- **Los términos y condiciones:** deben contener el detalle de las reglas y procedimientos de la prestación de los servicios por medio de los cuales se realiza o se apoya su atención, en caso de que cuenten con páginas web, o servicios vía aplicaciones.
- **Documentos de políticas de privacidad de los datos:** detalle del tipo de datos personales que serán objeto de tratamiento, la finalidad para la cual serán utilizados, los terceros a los que podrían comunicarse los datos, el tiempo de retención, y una cuenta a través de la cual se puedan ejercer los derechos de acceso, rectificación, y portabilidad de los datos.
- **Documentos de seguridad de la información:** con el detalle, al menos, de las reglas de gestión de perfiles y de las claves de acceso, y un contacto al cual comunicar

eventuales incidentes de seguridad a que pudieren verse expuestos los sistemas y servicios tecnológicos empleados en la provisión de las acciones y prestaciones de salud a distancia por TIC.

- **Retención y comunicación de las grabaciones:** Si el servicio considera la grabación de la atención y, en caso de contar con ello, el tiempo por el cual se conservarán los registros y posibles comunicaciones a terceros.
- El profesional deberá incluir siempre una explicación, en lenguaje sencillo y acorde a las necesidades de la persona que va a atender, de las limitaciones con que cuenta, de la misma forma en que lo informa en las consultas presenciales cuando sabe que no podrá resolver alguna situación. Esto debe hacerse al inicio de cada prestación de telemedicina.

2. Obtención del consentimiento

i. **Regla General:** La regla general a este respecto se encuentra en el artículo 14 inc. 5° de la ley N°20.584, el que dispone: *"El consentimiento informado del paciente para recibir prestaciones de salud digital se podrá otorgar en forma verbal, caso en el cual el prestador institucional e individual respectivo deberá registrar la aceptación o rechazo de la atención de salud mediante una* ***declaración escrita en formato papel o firmado a través de un sistema electrónico que garantice su autenticidad*** *de conformidad con lo dispuesto en la ley N° 19.799, dejándose registro en la ficha clínica de los resguardos adoptados para asegurar el derecho de información de la persona".* Tratándose de atenciones realizadas en el marzo de la investigación científica biomédica en personas humanas, además se deberá considerar lo previsto en la ley N° 20.120 y su reglamento.

   En este sentido, el reglamento sobre acciones vinculadas a la atención de salud a distancia indica que la aceptación de la modalidad de atención a distancia o su denegación podrá ser verbal o por escrito, y la circunstancia de la aceptación o rechazo se deberá registrar a través de un medio fidedigno. La aceptación de la modalidad de atención a distancia es requisito para la entrega o realización de la acción o prestación y conlleva el reconocimiento de la persona de contar con los medios necesarios para su otorgamiento.

   - **Consentimiento verbal:** En aquellos casos que no se requiera que el consentimiento se otorgue a través de documento escrito y firmado de puño y letra del paciente o de la persona bajo cuyo cuidado se encuentre, el profesional deberá dejar constancia en la ficha clínica del hecho de haberse otorgado y la identidad de la persona que lo presta.

     La aceptación o el rechazo de la atención mediante telemedicina deberá manifestada por la persona o del adulto bajo cuyo cuidado se encuentre. Se deberá dejar constancia en la ficha clínica de estas circunstancias. Si no se trata de un procedimiento invasivo bastará que el profesional consigne en la ficha el hecho de haberse otorgado o no el consentimiento respecto de la modalidad de atención, sin necesidad de que la persona firme algún documento que dé cuenta de ello. La constancia servirá como una forma de acreditar o probar el hecho en sí mismo en futuras fiscalizaciones o revisiones.
   - **Consentimiento expreso y por escrito:** Las prestaciones de salud que incluyen procedimientos invasivos, tales como *"intervenciones quirúrgicas, procedimientos diagnósticos y terapéuticos invasivos y, en general, para la aplicación de procedimientos que conlleven un riesgo relevante y conocido para la salud del afectado"*, como por ejemplo, la trombólisis en ataque cerebro vascular u otros similares, deberán contar con un consentimiento informado con un registro firmado por el paciente o por la persona

bajo cuyo cuidado se encuentre. Esto podrá realizarse a través de un registro manual o electrónico, debiendo en todo caso adoptarse las medidas que permitan verificar la identidad del otorgante y el paciente, los datos de la acción o prestación de que se trate y la suscripción a través de un medio idóneo, que minimice los riesgos de adulteración del documento, o suplantación de la identidad.

Sin perjuicio de lo anterior, se debe considerar que el artículo 15 de la Ley N° 20.584 establecen situaciones en las cuales no es necesario solicitar el consentimiento, debiendo dejarse constancia en la ficha clínica de los hechos que configuran alguna de las causales previstas.

3. Accesibilidad

La accesibilidad dice relación con la previsión de condiciones o medios que permitan que todas las personas tengan acceso a las acciones y prestaciones de telemedicina, con independencia de si han adquirido conocimientos o competencias específicas en el ámbito tecnológico. En lo que nos interesa, el artículo 12 del Decreto N° 6 de 2021 de MINSAL, prevé que *"Tratándose de personas que no dominen suficientemente las TIC, o que tengan otra condición que les impidan hacer uso adecuado de ellas, la acción o prestación podrá otorgarse de manera remota asistido por una persona de su confianza o, en su defecto, un profesional, técnico o administrativo que tenga las competencias necesarias para apoyar al paciente en los aspectos relativos a la operación de las tecnologías necesarios para la conexión"*, dejándose registro del acompañamiento en la ficha clínica.

En la ficha clínica deberá dejarse constancia de la persona que otorga la asistencia a que se refiere esta norma y del hecho de habérsele informado sobre el deber de confidencialidad que le asiste.

4. Proceso de atención

a. Identificación fehaciente de las partes del proceso de atención: (arts. 9 y 11 de la ley N° 20.584; artículos 14 y 16 decreto N°6, 2022, MINSAL)

i. **Identificación del prestador:** El/la profesional que participa de la acción o prestación debe ident ificarse antes del comienzo del procedimiento de que se trate. Adicionalmente, los prestadores institucionales e individuales deberán resguardar que los sistemas y aplicaciones utilizados muestren, desde su inicio y durante toda la atención, el nombre completo y apellidos del prestador individual y su función; el prestador institucional al que pertenece, si corresponde; y el correo electrónico o teléfono al que le podrán dirigir comunicaciones, en letra legible e idioma castellano o en un idioma que sea inteligible y de fácil comprensión para el paciente.

ii. **Supervisión docente:** En el caso de que en el otorgamiento de la acción o prestación se encuentre presente o que sea otorgada por alumnos en establecimientos de carácter docente asistencial, como también en las entidades que han suscrito acuerdos de colaboración con universidades o institutos reconocidos, se deberá contar con la supervisión de un médico u otro profesional de la salud que trabaje en dicho establecimiento y que corresponda según el tipo de prestación, informarse al paciente de la identidad del mismo y solicitar la autorización al paciente para que el estudiante participe de la acción o prestación. (arts. 8, 10 bis y 13 de la ley N° 20.584).

iii. **Identificación del paciente:** La identidad del paciente deberá verificarse a través de mecanismos idóneos. A estos efectos, el prestador deberá solicitar y consignar en la ficha clínica y demás sistemas de apoyo al proceso asistencial, la casilla o plataforma digital u otro

medio acordado con el paciente o la persona bajo cuyo cuidado se encuentre, la dirección de correo electrónico o número telefónico al cual se le deben dirigir las notificaciones en el marco de las acciones vinculadas a la atención de salud realizada a distancia por medio o apoyada en TI. Asimismo, se le debe informar que es de su responsabilidad mantener actualizada esta información de contacto.

iv. **Idoneidad del espacio físico para otorgar la prestación a distancia:** el profesional que otorgue la prestación telemática deberá adoptar las medidas que permitan que el espacio cumple con los requisitos para entregar una atención de salud, asegurando la confidencialidad de la prestación otorgada. A estos efectos, en el caso que durante la atención el paciente se encuentre en su domicilio, en el proceso de agendamiento se informará sobre la necesidad de que se conecte desde un espacio que le permita resguardar su privacidad y tranquilidad durante el proceso de atención.

b. Acceso a la información clínica del paciente: (art. 13 ley N° 20.584; arts. 15 y 16 del decreto N° 6 de 2021 de MINSAL; decreto N° 41 de 2012 de Minsal)

El personal que participa directamente en la atención de salud del paciente podrá acceder oportunamente a los datos personales contenidos en la ficha clínica que sean necesarios para la ejecución de las acciones para las cuales se encuentran habilitados por la normativa que les rija, con la finalidad de garantizar la continuidad del cuidado de la persona. De lo anterior se deriva la obligación de registro, interoperabilidad y portabilidad de la ficha clínica.

Para el acceso, el prestador deberá disponer de los medios que permitan al profesional el acceso oportuno a la información que consta en la ficha clínica, con independencia de que preste servicios en el mismo prestador institucional o uno diferente. A estos efectos, la norma prevé el derecho de la persona a la **Portabilidad de la ficha clínica** (arts. 12 y 13 de la ley N° 20.584; art. 15 inc.2 decreto N° 6 de 2021 de Minsal y ley N° 19.799). Conforme a estas normas, el titular de la ficha clínica, su representante legal o, en caso de fallecimiento del titular, sus herederos; o un tercero debidamente autorizado por este, podrán requerir la entrega de todo o parte de la información contenida en la ficha clínica, íntegramente, en un formato estructurado, de uso común y lectura mecánica, ya sea para portarlos o para transmitirlos a otro prestador que se indique en la solicitud.

El prestador está obligado a la entrega gratuita y sin dilaciones indebidas de una copia íntegra de la ficha clínica, en un formato estructurado, de uso común y lectura legible, que sea susceptible de ser portado a otro sistema de ficha clínica, o bien transmitirlos a otro prestador que se indique en la solicitud. En caso de que la información se requiera para ser proporcionada a otro prestador, este requisito se cumplirá con la entrega de la información necesaria para que el prestador autorizado pueda acceder de manera remota a la ficha clínica del paciente y extraer la información necesaria para garantizar la continuidad del cuidado del paciente.

c. Registro en la ficha clínica: (arts. 12, 14, 31, 37, 39 de la ley N° 20.584; art. 7, 8, 9, 12, 13, 16 del decreto N° 6, de 2021 de MINSAL y decreto 41 de 2012, ambos de Minsal)

Los prestadores están sometidos a la misma obligación de registro de las acciones y prestaciones de salud que contempla la normativa sanitaria respecto de la modalidad presencial. Para estos efectos, el profesional que la otorga deberá contar con un perfil de acceso seguro, al sistema de gestión de las fichas que emplee el prestador institucional que corresponda.

d. Entrega al paciente del informe y registro de atención (artículos 10 Ley N°20.584, artículo 16 del decreto N° 6, de 2021 de MINSAL)

Al término de la atención, el prestador, por medio de una casilla o plataforma digital u otro medio acordado con el paciente o la persona bajo cuyo cuidado se encuentre, debe hacer entrega de un documento que contenga una copia del informe y registro de la atención, que incluya la identificación del paciente, diagnóstico o hipótesis diagnóstica, las indicaciones dadas al paciente, y la identificación del prestador individual que realizó la atención. Para estos efectos, el profesional solicitará al paciente o la persona bajo cuyo cuidado se encuentre, y consignará la dirección de correo electrónica válida y vigente o, en su defecto, o algún otro medio al cual se le podrá dirigir este documento además de las otras notificaciones a que se dé lugar en el marco de las acciones vinculadas a la atención de salud realizada a distancia por medio o apoyada en TIC. Asimismo, se debe informar al paciente o a la persona bajo cuyo cuidado se encuentre que es su deber mantener actualizada esta información de contacto en caso de que cambie.

En la ficha clínica se dejará constancia tanto de la información de contacto como del hecho de haberse remitido el documento respectivo.

e. Notificación de Enfermedades Transmisibles de Declaración Obligatoria y su Vigilancia. (art. 19 del decreto N° 6, de 2021 de MINSAL; decreto supremo N° 7, de 2019, de MINSAL)

En aquellos casos que proceda realizar una notificación obligatoria, en los términos de lo previsto en los artículos 20 y siguientes del Código Sanitario y del decreto supremo Nº 7, de 2019, del Ministerio de Salud, que aprueba el reglamento sobre notificación de enfermedades transmisibles de declaración obligatoria y su vigilancia, la notificación se realizará a la autoridad sanitaria más próxima al domicilio del paciente sobre quien se informa, a través del medio seguro más expedito.

5. Supresión o cancelación de datos

La ley impone el deber de conservación de la ficha clínica por los prestadores, por el término de al menos 15 años contados desde la última atención. Cuando proceda, el prestador debe adoptar procedimientos de supresión, cancelación o destrucción de datos que hayan devenido en caducos adecuados al carácter sensible de la información, debiendo dejar constancia de los distintos pasos y resultados obtenidos.

Los dispositivos digitales y magnéticos que se descarte deben ser sometidos a procedimientos de formateo seguro antes de ser descartados. Si se destruyen físicamente dispositivos de almacenamiento, ello se debe hacer de manera segura, verificando que los datos no sean recuperables. Esto podría implicar la trituración de discos duros o la eliminación segura de medios físicos.

En los procesos de digitalización de información queda prohibido destruir o descartar los originales sin la autorización respectiva del responsable del activo.

6. Otras medidas organizativas que debe adoptar el prestador

- **Cláusulas contractuales asociadas al cumplimiento de condiciones legales de tratamiento de datos:** Los contratos que emplee el prestador en sus procesos internos y externos deben contener la prohibición de uso de la información más allá de las necesidades asociadas al cumplimiento y finalidad del contrato, previendo que el incumplimiento de esta obligación configura un incumplimiento grave de las obligaciones que impone el contrato.

- **Auditabilidad de procesos, sistemas y plataformas:** Los prestadores deben prever en sus contratos con proveedores y disponer en sus procesos internos la realización de auditorías internas o externas de seguridad y que se generen y conserven las evidencias correspondientes.
- **Certificaciones de seguridad:** Dada la criticidad de los servicios y sensibilidad de los datos sanitarios, el prestador deberá procurar que los proveedores que les procuren los servicios tecnológicos requeridos para el otorgamiento de prestaciones de salud a distancia y telemedicina cuenten con certificaciones acordes a la criticidad de la información o los procesos que soporten, prefiriendo aquellos que cuenten con el nivel más alto de certificación de acuerdo con el estándar generalmente aceptado al momento de la contratación.
- **Mantenciones normativas:** Los contratos con proveedores deben contener cláusulas que prevean la adaptación de los sistemas a las exigencias que impongan los cambios regulatorios respecto de los procesos clínicos, de gestión documental, tratamiento de datos u otros aspectos técnicos relevantes para el cumplimiento normativo a que está sujeto el prestador.
- **Seudonimización de datos en servicios en nube:** Los procedimientos de gestión de datos sensibles deben considerar la aplicación de técnicas de seudonimización de datos sensibles de personas naturales (datos sensibles), manteniendo en el servidor local y con acceso controlado, los códigos que permitan la reidentificación de los datos. En el caso datos confidenciales que no sean susceptibles de seudonimización deberán aplicarse técnicas de encriptación que permitan asegurar que no serán accedidos ilegítimamente.
  - **Pruebas de seguridad:** El prestador debe realizar pruebas y ejercicios regulares de recuperación de datos personales para asegurar que el plan de contingencia funcione según lo previsto y para entrenar al personal en su implementación, asegurando la continuidad en la prestación de servicios a la población que atiende. El plan de pruebas debe considerar herramientas de detección y prevención de intrusiones (IDS/IPS) para el monitoreo de patrones de comportamiento usando modelos basados en reglas, heurísticos o de comportamiento para detectar anomalías en la actividad que pueden presentar riesgos.
  - **Evaluación de riesgos y análisis de impacto en el negocio (BIA):** Para identificar amenazas potenciales y sus efectos en las operaciones y, tratándose de procesamiento de datos, para identificar efectos adversos de los procesamientos de datos que se realizan respecto de los derechos de las personas.

B. Aspectos relativos a las plataformas y sistemas

1. Acreditación (artículo 10 bis de la ley Nº 20.584)

Las plataformas tecnológicas empleadas en las acciones y prestaciones de salud digital, así como las que almacenan y tratan datos personales, deberán estar acreditadas en cuanto al cumplimiento de las normas y estándares técnicos que establezca el Ministerio de Salud a través de un reglamento y las normas técnicas respectivas. Los estándares técnicos y administrativos de acreditación se definirán en un reglamento del Ministerio de Salud.

Los estándares técnicos fueron establecidos en el decreto Nº6 de diciembre de 2022, de MINSAL. En esta norma técnica se detallan las condiciones y requisitos que debieran considerarse en la implementación de las plataformas y sistemas, en atención a su impacto directo en el cumplimiento de los estándares de calidad del otorgamiento de la acción o prestación de salud a distancia, a través de telemedicina.

2. Reglas aplicables al tratamiento de datos personales (artículo 12 de la ley N° 20.584; artículo 16 decreto Nº 6, 2022, MINSAL)

De acuerdo con el artículo 12 de la ley N° 20.584, 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 fueron sometidas las personas, será considerada como dato sensible, de conformidad con lo dispuesto en la ley N° 19.628. De ello se deriva que todos los sistemas informáticos y plataformas de apoyo a las acciones de telemedicina deban resguardar la confidencialidad de la información y que los profesionales que accedan a los datos queden sujetos al deber de reserva o secreto. Adicionalmente, se deberán adoptar las siguientes medidas técnicas y organizativas:

a. Privacidad desde el diseño

Que un sistema sea diseñado en base a reglas de privacidad implica el cumplimiento de la normativa marco de protección de datos, prevista en la ley N° 19.628 y las obligaciones especiales previstas en la normativa sanitaria, especialmente en la implementación de medidas técnicas que den satisfacción a las obligaciones de confidencialidad, protección de la privacidad y de los datos personales del paciente.

b. Responsabilidad demostrable: (art. 3° ley N° 20.584)

El prestador deberá prever mecanismos y medios que le permitan contar con evidencias del cumplimiento de las obligaciones que emanan de la normativa de protección de datos. A vía ejemplar, los contratos con procesadores de información y con proveedores tecnológicos deberán incluir todas las instrucciones y salvaguardas que permitan resguardar los derechos de los titulares de datos, incluyendo la obligación del proveedor de cumplir y hacer cumplir estas obligaciones por parte de sus colaboradores o aliados. El contrato correspondiente deberá además contener todas las instrucciones relativas a la gestión de los archivos y datos personales que permitan resguardar la integridad, disponibilidad y confidencialidad de la información del paciente en los términos previstos en los artículos 5 y 7 de la ley Nº 20.584 y 10 de la Nº 19.628.

c. Protección extendida (artículos 12 y 13 Ley 20.584; 101 del Código Sanitario; artículos 10 al 15 decreto Nº6, 2022, MINSAL)

Las aplicaciones, sistemas y servicios de comunicaciones que soporten las acciones y prestaciones de salud a distancia realizadas a través de TIC, deberán garantizar la confidencialidad, respeto a la privacidad, y protección de los datos personales de los pacientes, según la normativa vigente. Esta obligación se extiende a toda la información relativa a la salud de la persona y los documentos en los cuales ésta conste, tales como exámenes de laboratorio o imágenes y sus respectivos informes, las prescripciones farmacológicas, las licencias médicas, los formularios de notificación de patologías GES, etc.

En aquellos casos que se comunique o transfiera la información de salud de un paciente en virtud de las obligaciones de portabilidad e interoperabilidad, la obligación de resguardo de la información recaerá en el prestador receptor de los datos deberá. El deber de confidencialidad o reserva se mantendrá vigente de manera indefinida.

d. Gestión de riesgos de privacidad

Los riesgos de privacidad incluyen los accesos indebidos, fugas, daños o pérdidas de información. La gestión de riesgos de privacidad supone el identificar, documentar y mitigar los efectos de un eventual incidente que afecte la privacidad de la información del paciente.

Estas medidas podrán ser técnica organizativas y contractuales, destinadas a minimizar los riesgos de quiebres de seguridad y su impacto en el proceso de atención y en el resguardo de la información confidencial del paciente.

Adicionalmente, tratándose de prestadores del sector público y aquellos que realicen acciones y prestaciones de salud financiada con fondos públicos están obligados a notificar al Comité de Seguridad de la Información del Nivel Central del Ministerio de Salud, los incidentes que puedan afectar la seguridad de los datos y sistemas que se empleen en las acciones y prestaciones de salud en general, incluyendo aquellas que se realizan a distancia a través de tecnologías de la información y comunicaciones.

El tratamiento de datos en la nube debe garantizar la seguridad de los datos, previéndose en los contratos las obligaciones y resguardos que permitan cumplir con esta obligación.

e. Resguardo de la calidad de datos

La calidad de la información clínica es esencial para garantizar la continuidad del cuidado de los pacientes. Cada uno de los profesionales que ingresen al sistema de registro deberá ser capacitado en las reglas semánticas y sintácticas previstas para resguardar la calidad sustantiva y formal de la información que conste en dichos sistemas.

A este respecto, la estandarización de datos es esencial para garantizar que los sistemas y aplicaciones puedan comunicarse de manera efectiva y que los datos se compartan de manera coherente y segura en diversos contextos de la atención médica, porque garantiza que los datos se presenten de manera uniforme, manteniendo el contexto y el significado de la información, lo que facilita su comprensión y evita confusiones. Esto es importante en la atención médica, donde la interpretación errónea de datos podría tener graves consecuencias.

En este ámbito, estándar de interoperabilidad HL7® FHIR® (Fast Healthcare Interoperability Resources) representa una solución robusta y eficiente para enfrentar los desafíos actuales en el ámbito de la salud digital por lo que MINSAL se encuentra trabajando en la elaboración de guías de implementación que serán puestas a disposición de la comunidad.

Las guías de implementación estarán disponibles en https://interoperabilidad.minsal.cl/ y en https://deis.minsal.cl/ junto con los plazos de implementación progresiva, los cuales serán individualizados por proceso y organización. Esto permitirá minimizar interrupciones en la prestación de servicios de salud y garantizar una transición gradual hacia sistemas más interoperables y eficientes.

En otro ámbito, la obligación de resguardo de la calidad de los datos incluye el deber de mantener respaldos funcionales en un lugar seguro y asequible y que el plan de contingencia contemple la restauración de datos oportuna en el caso de ocurrir un incidente que pueda afectar la integridad, autenticidad o disponibilidad de la información clínica.

f. Cumplimiento de los principios de protección de datos personales

i. **Finalidad:** El tratamiento de datos personales de salud de la persona debe tener un objetivo sanitario definido, ya sea asistencial o en el ámbito de la investigación científica biomédica.

En este ámbito, el artículo 10 del decreto N°6, 2022, MINSAL, dispone expresamente que *"En el desarrollo de las acciones vinculadas a la atención de salud realizada a distancia, podrán incorporarse técnicas y métodos de procesamiento de datos y análisis de información, siempre que tengan un objetivo sanitario definido y cumplan con la presente normativa, la regulación vigente en Chile en materia de tratamiento de datos de carácter personal y datos sensibles, y los lineamientos que dicte el Ministerio de Salud sobre la materia en cumplimiento de lo dispuesto en el artículo 5 inciso final de la ley Nº 20.584".*

ii. **Seguridad:** Los datos clínicos transmitidos y almacenados deben contar con una protección sólida, que incluya medidas de seguridad como la encriptación, la autenticación y el control de acceso. A lo largo de todo el proceso asistencial mediante telemedicina es fundamental implementar las medidas técnicas y organizativas que permitan minimizar la ocurrencia e impacto de incidentes de seguridad. Adicionalmente, el prestador deberá mantener operativos mecanismos de control de acceso para asegurar que solo el personal autorizado pueda acceder a la información médica y los sistemas de registro, en los siguientes términos:

- **Autenticación:** Se deben implementar sistemas de autenticación fuertes, con contraseñas robustas y con a lo menos con autenticación de dos factores, para asegurar que solo los usuarios autorizados puedan acceder a la información. Se deben utilizar protocolos de autenticación seguros (como por ejemplo OAuth 2.0 o superior) para permitir a los pacientes y profesionales de la salud acceder de manera segura a las plataformas de telemedicina. Para la autenticación de prestadores el Ministerio podrá implementar autenticación a través de clave única.
- **Acceso:** El acceso a plataformas de telemedicina debe requerir autenticación mediante credenciales únicas y seguras, tanto para los profesionales de la salud como para los pacientes. Se deben implementar medidas para prevenir el acceso no autorizado a los datos clínicos, como acceso basado en roles, limitando el acceso a la información según las responsabilidades de los usuarios, con el acceso de estos limitado a la información relevante para realizar sus funciones.
- **Perfilamiento:** Se deberán considerar medidas que permitan fortalecer la seguridad relacionada con el perfilamiento de usuarios e identidad digital en la organización, tales como las relacionadas con el control de acceso basado en roles, el registro y monitorización de las actividades de inicio de sesión, incluidos los intentos de acceso fallidos; la implementación de sistemas de gestión de identidad (IDM para gestionar de manera centralizada la identidad de los usuarios, la autenticación y la autorización).
- **Actualización:** Deben realizarse revisiones regulares de los permisos de acceso para garantizar que los usuarios necesitan efectivamente todas las autorizaciones que se les han otorgado.
- **Licitud:** El prestador deberá resguardar que sólo se traten datos respecto de los cuales tenga autorización legal o el consentimiento del titular o de su representante legal, si procede. Asimismo, deberá resguardar que los datos sólo se utilicen en el marco de la finalidad legítima informada. La comunicación o transferencia de datos sólo procede respecto de los profesionales que participan directamente en las acciones o prestaciones de salud del paciente que es titular de los datos. La transferencia internacional de datos sólo se encuentra autorizada a aquellos países que cuentan con un "nivel adecuado de protección".

3. Estándares de seguridad de la información en el otorgamiento de acciones y prestaciones a distancia y telemedicina (Artículo 3 de la ley Nº 20.584; artículos 7, 8 y 9 decreto Nº6, 2022, MINSAL)

A continuación, se proporcionan directrices técnicas que garanticen la protección de datos personales y de salud, tales como medidas de cifrado, almacenamiento seguro y transmisión de datos confidenciales; adopción de medidas que permitan al ecosistema nacional resistir de mejor forma a posibles amenazas y vulnerabilidades.

Asimismo, se busca dar lineamientos para identificar y abordar de manera proactiva los riesgos y amenazas de seguridad cibernética y tecnológica que puedan surgir en las prestaciones de salud a distancia y que permitan implementar medidas de seguridad efectivas y prácticas seguras en el ámbito de la telemedicina, de manera que tanto profesionales de la salud como pacientes puedan confiar en la integridad y confidencialidad de los datos.

Los estándares que se detallan a continuación se traducen en un conjunto de actividades diseñadas para alcanzar objetivos precisos en esta área, cuya finalidad principal es garantizar la confidencialidad, integridad y disponibilidad de la información:

a. **Gobernanza en Seguridad (artículo 3 de la ley Nº 20.584; art. 13 del decreto Nº6, 2022, MINSAL)**

   El artículo 3 de la ley Nº 20.584, en su inciso séptimo prevé que *"Será responsabilidad de los prestadores institucionales e individuales de salud que otorguen acciones de salud digital, utilizar medios técnicos que cumplan los estándares de seguridad que establezca el Ministerio de Salud en todas las etapas del tratamiento de datos, siendo responsables de todo daño que ocasionare el incumplimiento a dicho deber".* Conforme a esta norma legal, los prestadores de servicios de salud a distancia y telemedicina deben contar con procesos sólidos y estructuras adecuadas para gestionar y mantener la seguridad de la información de manera efectiva. Los prestadores deben contar con un oficial de seguridad de la información, que lidere la implementación y mejora continua del sistema de gestión de seguridad de la información y un comité de seguridad de la información que le permita gestionar el sistema de seguridad implementado.

b. **Diseñar, aprobar a implementar políticas y procedimientos de seguridad de la información (art. 13 del decreto Nº6, 2022, MINSAL)**

   Con independencia de que el prestador utilice capacidades propias o contrate plataformas y servicios técnicos a terceros, tal como señala el mismo artículo tres en su inciso octavo: *"No será eximente de responsabilidad que el prestador utilice a estos efectos medios de terceros, sin perjuicio de la responsabilidad del proveedor de servicios conforme a las reglas generales".*

   Esta norma es desarrollada en el artículo 8 del decreto Nº6, de 2022, de MINSAL, que obliga a los prestadores a establecer condiciones para asegurar la confidencialidad, disponibilidad y privacidad de la información de los pacientes, debiendo disponer de procedimientos específicos de aseguramiento de la confidencialidad, según la acción o prestación otorgada; contar con *"planes de gestión de riesgos de privacidad, que le permitan minimizar los riesgos asociados a quiebres de seguridad, especialmente si se teme que, de ello se haya derivado algún acceso o divulgación indebida, una alteración o modificación de los datos personales relativos a los pacientes".*

   Por lo tanto, el prestador debe implementar políticas y procedimientos claros y concisos que establezcan las condiciones de seguridad de los sistemas y las reglas que rigen aspectos tales como el acceso a la información, el uso aceptable de los sistemas, la gestión de contraseñas y todos aquellos aspectos que tengan implicancias en la usabilidad y acceso seguro a los sistemas y aplicaciones.

c. Implementar políticas de privacidad y tratamiento de datos personales (art. 13 del decreto N°6, 2022, MINSAL)

A continuación, el inciso noveno del artículo 3 establece que *"Para los efectos del tratamiento de datos personales, se entenderá que el prestador es el responsable de llevar los registros o bases de datos de los pacientes que se generen con ocasión de la gestión de los sistemas de apoyo a la salud, y los proveedores tendrán las responsabilidades propias de un mandatario, en los términos previstos en la ley N° 19.628 sobre protección de la vida privada"*. En cumplimiento de esta norma, los sistemas y plataformas del prestador deben contar con avisos de privacidad en que se consignen las bases de licitud del tratamiento de datos, el tipo de información que es objeto de tratamiento, las fuentes desde las cuales se recopilan los datos, las condiciones de almacenamiento, procesamiento y los destinatarios de la información, además de cumplir con las normas y principios que rigen para el tratamiento de datos sensibles.

d. Implementar controles de acceso y trazabilidad de las operaciones realizadas sobre los datos y sistemas

Los sistemas y plataformas del prestador deben estar diseñados con reglas de seguridad por defecto. Por lo tanto, deben contar con sistemas de control de acceso, perfilamiento de usuarios, registro y conservación de logs. Realizar auditorías internas o externas que les permita controlar el uso que se haga de los sistemas, e identificar de manera unívoca a los usuarios que accedieron y realizaron operaciones de tratamiento sobre los datos que son objeto de tratamiento. Para ello se deberán implementar cuentas nominadas y sistemas de auditoría de las sesiones de cada usuario que entre en interacción con el sistema.

Adicionalmente, el prestador debe implementar sistemas de gestión de los perfiles profesionales debe garantizar que cada uno de ellos, dentro del ámbito de sus competencias, tenga acceso eficaz y oportuno a la información que requieren, para cumplir su función dentro del proceso de atención al paciente.

e. Sistemas de ficha clínica diseñados para interoperar: (art. 13 de la ley N° 20.584)

El prestador debe utilizar sistemas y plataformas diseñadas para interoperar con otros sistemas necesarios para el otorgamiento de acciones y prestaciones de salud, propios o de terceros. El Ministerio de Salud se encuentra trabajando en un reglamento y norma técnica que determinará los estándares que sean necesarios para garantizar la integración e integridad de los datos, interoperabilidad, disponibilidad, autenticidad y confidencialidad de la información que conste en la ficha clínica, además de las condiciones o resguardos administrativos que sean necesarios para tales efectos. En este ámbito, se prevé que los sistemas deberán obedecer a lógicas de neutralidad tecnológica, en el sentido que la ficha y los sistemas que la soportan esté diseñada e implementada para interoperar desde el punto de vista semántico y sintáctico, tanto a nivel de datos, sistemas y redes de comunicaciones.

f. Transmisión segura de la información clínica. (art. 13 de la ley N° 20.584; art. 7 del decreto Nº 6 de diciembre de 2022, MINSAL)

Los prestadores deberán contar con procedimientos y medios que garanticen que toda comunicación de datos clínicos sea encriptada y que se utilicen protocolos de seguridad confiables. Al respecto, se deberán adoptar las siguientes medidas de seguridad:

- **Transmisión segura:** Para efectos de garantizar la integridad y confidencialidad de los datos durante la transmisión, los sistemas y plataformas aplicables al ámbito de la salud deberán utilizar protocolos de seguridad validados actualizados y vigentes, tales como

TLS (Transport Layer Security) para encriptar la comunicación entre dispositivos. Los servidores web deben admitir conexiones seguras bajo l protocolo de transferencia de hipertexto seguro (HTTPS).

- **Encriptación de Datos:** En la comunicación de los datos de salud de las personas, el prestador debe implementar mecanismo encriptación fuertes, de extremo a extremo, tales como AES (Advanced Encryption Standard),128 bits y superior (192 y 256) o algoritmo de HASH de la familia SHA-2 o 3 (Secure Hash Algoritm) o superior.
- **Comunicación por videoconferencia:** Los sistemas de videoconferencia que utilicen los prestadores deben contar con un protocolo seguro de acceso de usuario, que minimice los riesgos de intrusiones ilegítimas o suplantaciones. En la comunicación de video y voz se debe implementar cifrado robusto, que asegure que las conversaciones sean inaccesibles para terceros no autorizados y mecanismos de verificación de la integridad de los datos, evitando manipulaciones no deseadas durante la transmisión.

  En el enrutamiento de mensajes se debe implementar un protocolo de identificación de origen y destino que permita validar a lo menos la identidad del paciente y el profesional de la salud. El sistema deberá contar con servicio de registro y custodia segura de las videoconferencias para su posterior auditoría.

g. Plan de gestión de seguridad de la información: (artículos 8 y 9, decreto Nº 6 de 2022 de MINSAL)

La seguridad de los documentos electrónicos se encuentra regulada por la ley N° 19.799 de documentos y firmas electrónicas y su normativa complementaria. En su aplicación a la gestión de los documentos asociados a las acciones y prestaciones de salud, los prestadores deberán adoptar las siguientes medidas:

- **Almacenamiento Seguro:** Los sistemas de almacenamiento de datos clínicos deben ser servidores seguros y protegidos. Las políticas de respaldo deben considerar el restablecimiento de máquina, servicios y datos. Las pruebas de sistema deberán realizarse en máquinas independientes de aquellas que se emplean para los sistemas en producción. Se debe habilitar la encriptación de disco completo en los dispositivos utilizados para acceder a la plataforma de telemedicina.
- **Firewalls y Filtros:** Los sistemas deben estar protegidos con firewalls de próxima generación o superior para inspección profunda de paquetes y sistemas de filtrado para controlar y monitorear el tráfico entrante y saliente en busca de amenazas y para proteger los sistemas de telemedicina contra ataques externos y malwares, e implementar soluciones de detección y prevención de intrusiones (IDS/IPS) para monitorear y bloquear actividades maliciosas en la red. Se debe además utilizar segmentación de red para aislar los sistemas de telemedicina de otras redes y segmentos de la organización. Adicionalmente, se deberán configurar reglas de firewall para restringir el tráfico no deseado y prevenir ataques DDoS, e incluir un Web Application Firewall (WAF) para proteger aplicaciones web contra diversas amenazas.
- **Uso seguro de Internet:** El prestador deberá implementar medidas de seguridad que protejan tanto dispositivos como datos clínicos. Con este objetivo, se debe promover la utilización de redes Wi-Fi seguras y evitar el uso de conexiones a redes públicas sin protección, así como la navegación consciente, evitando sitios web no seguros o phishing. Se deben utilizar conexiones seguras (HTTPS) para proteger la información transmitida y mantener antimalware, sistema operativo, navegadores web y otras aplicaciones actualizadas para corregir vulnerabilidades de seguridad.

- **Actualizaciones y Parches:** Se deben de mantener al día todos los sistemas y aplicaciones con las últimas actualizaciones y parches de seguridad para mitigar vulnerabilidades conocidas y tener un proceso estructurado para identificar, evaluar y aplicar parches de seguridad de manera oportuna.
- **Seguridad del Dispositivo:** Todos los dispositivos utilizados para acceder a las plataformas y sistemas empleados en las acciones y prestaciones de salud a distancia y telemedicina estén protegidos con software de seguridad actualizado y configuraciones seguras (Protección de Dispositivos y Endpoints), como protección contra malware, configuración de bloqueo remoto y borrado de datos en caso de pérdida o robo de dispositivos.
- **Control de Dispositivos Móviles:** Se deben utilizar dispositivos móviles dotados de las medidas de seguridad corporativas para acceder a sistemas de telemedicina, como la gestión de dispositivos móviles (MDM) o similar, para proteger los datos en caso de pérdida o robo.
- **Evaluaciones de Seguridad:** El prestador debe realizar pruebas de penetración regulares y evaluaciones de seguridad para identificar posibles vulnerabilidades y áreas de mejora a sus aplicaciones de telemedicina e infraestructura tecnológica. Además, se debe llevar un registro de las evaluaciones y mitigaciones realizadas a los sistemas.
- **Auditorías y Registros:** Se debe establecer la capacidad de registrar y auditar las actividades de usuario para rastrear cualquier actividad sospechosa o inusual. Se deberá conocer quién se conecta, a qué hora y desde que dirección IP, además de monitorizar de forma proactiva y continua la seguridad de la infraestructura tecnológica.
- **Monitoreo Continuo:** Se deben implementar sistemas de monitoreo de seguridad para detectar y responder rápidamente a cualquier actividad sospechosa, aumentar la capacidad de vigilancia de las redes y los sistemas e implementar sistemas de registro de eventos y actividades en tiempo real para capturar y almacenar información detallada sobre las interacciones y cambios en los sistemas.
- **Registro de Actividades (LOG):** Debe mantenerse un registro detallado de todas las actividades relacionadas con la prestación de atención de salud mediante telemedicina, incluyendo fechas, horas y detalles de las interacciones que MINSAL establezca que integran el Conjunto Mínimo Básico de Datos.

  Se deben mantener registros detallados de las actividades realizadas en el sistema, incluyendo quién accedió, cuándo y qué acciones se llevaron a cabo. Esto permite rastrear cualquier posible incidente de seguridad.
- **Auditorías de Seguridad Periódicas:** Se deben realizar auditorías regulares para evaluar el cumplimiento de las medidas de seguridad de la información, la adecuada protección de los datos médicos y la identificación de áreas de mejora.
- **Gestión de incidentes de seguridad:** El prestador debe implementar procedimientos para la comunicación y manejo de incidentes de seguridad de la información, tanto a nivel interno como al Comité de Seguridad de la Información (CSI) del Ministerio de Salud, a nivel central, dentro de las 72 horas siguientes al momento en que el incidente haya sido detectado y a los pacientes cuya información pudo verse comprometida.

  El sistema de seguridad debe incluir un plan de respuesta a incidentes que detalle cómo abordar y mitigar eventuales amenazas de seguridad, así como cómo notificar a las partes

afectadas en caso de una brecha de seguridad. Los procedimientos de comunicación deben establecer una ruta de escalamiento eficaz y priorizada para los incidentes, para que la gestión de crisis y los planes de gestión de continuidad de negocio puedan estar involucrados en las circunstancias y momento correctos. El prestador deberá contar con un equipo de respuesta a incidentes que pueda evaluar y mitigar amenazas de seguridad de manera efectiva.

- **Identificación y evaluación periódica de riesgos de seguridad de información y tecnológicos.** El prestador debe mantener un enfoque proactivo en la seguridad de la información y tecnológica, enfocado a la educación y prevención de incidentes de seguridad.
- **Implementación de medidas de mitigación adecuadas.** El prestador deberá evaluar los riesgos de seguridad y tomar acciones para reducir o controlar sus efectos, tales como respaldos funcionales que permitan restablecer los datos y sistemas.
- **Plan de recuperación de desastres y medidas de contingencia:** El prestador debe asegurar la operación y la continuidad de las plataformas y sistemas que apoyan los modelos de atención. Para esta finalidad deberá implementar al menos las siguientes medidas:
  - » **Plan de Continuidad del Negocio (BCP):** Conjunto de medidas y responsables asociados a los pasos a seguir para continuar brindando acciones y prestaciones de salud en caso de incidentes de seguridad que interrumpan o degraden los servicios tecnológicos, incluyendo procedimientos para la restauración de servicios y la reanudación de operaciones.
  - » **Recuperación de Desastres (DRP):** Conjunto de medidas y responsables asociados a los pasos a seguir para la recuperación de sistemas y aplicaciones en caso de eventos graves, como fallos en el hardware, desastres naturales, etc.
  - » **Respaldo de Datos:** Políticas y procedimiento de realización, custodia segura, auditoría (test) y acceso eficiente a copias de seguridad regulares (backup), aptas para la recuperación de servicios en caso de pérdida de datos.
  - » **Documentación de Procesos Críticos:** El prestador debe documentar los procesos críticos del proceso de atención por telemedicina, incluidos los procedimientos de atención al paciente, comunicaciones y gestión de datos que faciliten la recuperación en caso de que el personal clave no esté disponible.
  - » **Infraestructura Redundante:** Debe considerarse la implementación de infraestructura redundante, como servidores y conexiones de red duplicadas, para reducir el impacto de posibles fallas.
  - » **Restauración Rápida:** Debe asegurarse que los sistemas críticos puedan ser restaurados rápidamente después de una interrupción. Esto puede implicar la implementación de imágenes de disco y copias de seguridad que puedan ser utilizadas para una recuperación rápida.
- **Herramientas de evaluación de seguridad de la plataforma** que se conecte con los servicios en la nube a través de una API para evaluar no sólo los activos desplegados en la nube, sino también que la configuración de la nube responda a los objetivos institucionales.

X. SANCIONES Y CUMPLIMIENTO LEGAL

El incumplimiento de esta norma técnica puede conllevar sanciones legales y disciplinarias según las regulaciones vigentes indicadas en la presente normativa.

Los profesionales de la salud y personal administrativo son responsables de garantizar la seguridad de la información en la prestación de atención de salud mediante telemedicina y del cumplimiento a las normas establecidas, con independencia del régimen contractual en base al cual desarrollen sus labores, o que desarrollen las labores a través de personal de su dependencia o subcontratación.

XI. GLOSARIO DE SEGURIDAD DE LA INFORMACIÓN

Video llamada	Es un modo de videoconferencia que involucra a dos usuarios que pueden verse y escucharse al mismo tiempo. Durante una videollamada los usuarios pueden compartir archivos y otro contenido multimedia, por ejemplo, compartir su escritorio, intercambiar mensajes de texto y usar herramientas de colaboración proporcionadas por la videoconferencia. La videollamada debe ser el canal preferente para la realización de atenciones a distancia, dejando el canal telefónico para aquellos casos donde no es posible realizar una videollamada.
Profesionales de la salud	Individuos autorizados y capacitados para brindar atención médica.
Paciente	Persona que recibe atención de salud a través de telemedicina.
Activos de Información	Toda información o recurso relacionado para la creación, almacenamiento, gestión o transmisión de dicha información. Podrán ser activos materiales (RRHH especializados, aparatos, equipos, redes, instalaciones, soportes y sistemas de almacenamiento) o intangibles (datos, aplicaciones, sistemas operativos, bases de datos, imagen, reputación, marcas de la organización).
Autenticación	Proceso utilizado en los mecanismos de control de acceso con el objetivo de verificar la identidad de un usuario, dispositivo o sistema mediante la comprobación de credenciales de acceso.
Anonimización	Proceso de convertir los datos en una forma en que no se pueda identificar a la persona a la cual se refieren.
Pseudoanonimización	Proceso para sustituir un atributo por otro en un registro, de tal forma que a pesar de que siga existiendo la posibilidad de vincular a la persona de manera indirecta con el conjunto de datos origen, se dificulta tal acción.
Ciberataque	Cualquier incidente cibernético, provocado deliberadamente y que afecte a un sistema informático.
Ciberespacio	El ciberespacio es un ambiente complejo resultante de la interacción de las personas, el software y los servicios de Internet, soportados éstos por el hardware y las redes de comunicaciones (ISO 27.032).
Ciberincidente	Todo evento, que afecte a un recurso disponible en, o expuesto al ciberespacio, que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los sistemas o datos informáticos almacenados, transmitidos o procesados, o los servicios correspondientes ofrecidos por dichos sistemas y su infraestructura, que puedan afectar al normal funcionamiento de estos.

Ciberseguridad	Conjunto de acciones destinadas a la prevención, mitigación, investigación y manejo de las amenazas e incidentes sobre los activos de información, datos y servicios, disponibles o expuestos al ciberespacio, así como para la reducción de los efectos de estos y del daño causado antes, durante y después de su ocurrencia.
Ciberconfidencialidad	Atributo de seguridad que consiste en que los datos deben únicamente ser accedidos por el personal autorizado a tal efecto.
Continuidad de Servicios	Adoptar las medidas que permitan proveer un nivel mínimo de servicio, entendiendo por esto las prestaciones propias del sistema, reduciendo el riesgo de eventos que puedan dar lugar a una interrupción o inestabilidad en las operaciones de la entidad, manteniendo niveles aceptables y propiciando la recuperación de los servicios de las tecnologías de la información (TI) en el menor tiempo posible.
Datos Personales o datos de carácter personal	Los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, con independencia de su soporte.
Datos Sensibles	Datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
Disponibilidad	Es la característica de la información contenida en la historia clínica que permite que esta sea accesible y utilizable cuando se requiera.
Gestión de Incidentes	Procedimientos para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante ésta.
Incidente	Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información (véase también ciberincidente).
Infraestructura Critica	Las instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. Se entiende por este concepto la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud.
Integridad	Atributo de seguridad que se atribuye a un sistema de información o a los datos que alberga, dando cuenta de su correctitud y completitud de los datos, información y sistemas, de forma que sea factible garantizar que los datos permanezcan intactos, que se puedan buscar y recuperar durante el transcurso de su ciclo de vida. La falta de Integridad considera todas las posibles causas de modificación, incluyendo fallos software y hardware, eventos medioambientales e intervención humana.
Intercambio	Los datos clínicos relevantes de la historia clínica deben estar disponibles a través de medios electrónicos con mecanismos de seguridad y privacidad que permitan la entrega a quién legítimamente tenga la facultad de acceder a ellos.

Oportunidad	Disposición permanente de los datos clínicos relevantes interoperables de la historia clínica para la continuidad de la atención y la toma de decisiones.
Protección de los activos de información	Adoptar las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos.
Resiliencia	Capacidad de los sistemas, equipos o redes para seguir operando pese a estar sometidos a un incidente o ciberataque, aunque sea en un estado degradado, debilitado o segmentado. Así como, la capacidad de restaurar con presteza sus funciones esenciales después de un incidente o ataque de modo de recuperarse con rapidez de una interrupción, por lo general con un efecto reconocible mínimo.
Riesgo en Ciberseguridad	Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una de las amenazas antes mencionadas que produzca un impacto en términos de operatividad, o de integridad, confidencialidad o disponibilidad de datos.
Seguridad	Los datos que se generan o se consultan se deben manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta o uso no autorizado.
Seguridad de la información	Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.
Tratamiento de Datos	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.
Vulnerabilidad o brecha informática	Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.
Uniformidad	Los conceptos, definiciones y nomenclaturas son únicos, con el fin de permitir la integración de la información y la comparación de resultados.

XII. VIGENCIA Y ACTUALIZACIÓN

Esta normativa entrará en vigor a partir de su publicación oficial y deberá ser revisada y actualizada de manera periódica cada año calendario, para garantizar su pertinencia y eficacia en el entorno cambiante de la atención médica y tecnológica.

XIII. BIBLIOGRAFÍA

1. Constitución Política de la República de Chile.
2. Corfo, Fundamentos para los Lineamientos para el desarrollo de la Telemedicina y Telesalud en Chile Bien Público Estratégico 18BPE-93834 Corfo InnovaChile - Segunda Edición.
3. Decreto N° 6, 2022, Ministerio de Salud, Reglamento sobre acciones vinculadas a la atención de salud realizada a distancia.
4. Decreto Supremo N° 83, 2005, Aprueba norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos;
5. Decreto N°273, 2022, Ministerio del Interior y Seguridad Pública, Establece obligación de reportar incidentes de ciberseguridad.
6. Decreto N° 779, de 2000, que Aprueba Reglamento del Registro de Bancos de Datos Personales a cargo de organismos públicos.
7. Directrices de la Organización Mundial de la Salud (OMS) sobre seguridad y privacidad en la telemedicina para ayudar a los países a desarrollar políticas y regulaciones adecuadas.
8. ENISA Guidelines de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) que ofrece pautas específicas para la seguridad de la información en la telemedicina en la Unión Europea.
9. Guía de Telemedicina Seminario del Lanzamiento: Propuesta Colaborativa para Impulsar la Telemedicina en Chile. Julio 2022
10. Instructivo Presidencial N° 8, 23 de octubre de 2018, que imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado.
11. Instructivo Presidencial N° 1, 19 de febrero de 2018, Instructivo Presidencial que entrega directrices sobre la evaluación y adopción preferente de servicios en la nube por parte de los órganos de la administración central del Estado;
12. Ley N° 21.541, que modifica N° 20.584."Regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud". Disponible en https://www.bcn.cl/leychile/navegar?idNorma=1039348
13. Ministerio de Salud, "Estrategia Nacional de Salud para el cumplimiento de los objetivos Sanitarios de la década 2021-2030".
14. NIST SP 800-66 publicado por el Instituto Nacional de Estándares y Tecnología (NIST) de los EE. UU., ofrece directrices sobre la seguridad de la información para la telemedicina.
15. OMS, "58a Asamblea Mundial de la Salud". 16-may-2005.
16. OPS Experiencias nacionales en telesalud: Preguntas orientadoras para visitas en terreno. Disponible en https://iris.paho.org/handle/10665.2/57027 ·
17. Programa Nacional de Telesalud en el contexto de Redes Integradas de Servicios de Salud Subsecretaría de Redes Asistenciales Guías de Buenas Prácticas Documentos Hospital Digital, APS, DIGERA.
18. "Programa de Gobierno Michelle Bachelet 2014-2018". 2013.
19. Resolución Exenta N° 489, 2022, Consejo para la Transparencia, Aprueba procedimiento para la tramitación de solicitudes de ejercicio de derechos de la ley N° 19.628, sobre protección a la vida privada;
20. Subsecretaria de Redes Asistenciales, "Glosa 06. Lista de espera No GES y garantías de oportunidad ges retrasadas". 2017.


Ministerio de
Salud
Gobierno de Chile