POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

DXMédica

Dato	Información
Documento	Política de Protección de Datos Personales
Organización	DXMedica SA
Versión	0.9
Estado	Borrador para revisión y aprobación
Autoridad de aprobación	Dr. Pablo Lespi
Referente operativo y tecnológico	Ladislao Potocki
Fecha de elaboración	10 de Marzo de 2026
Frecuencia de revisión	Anual o ante cambios relevantes

---

1. Objeto

La presente Política de Protección de Datos Personales tiene por objeto establecer los principios, responsabilidades y reglas generales que deberá aplicar el Laboratorio DXMédica para la recolección, registro, utilización, consulta, modificación, conservación, comunicación, transferencia y eliminación de datos personales.

Su finalidad es proteger la privacidad, intimidad y confidencialidad de los pacientes, profesionales, empleados, proveedores y demás personas cuyos datos sean tratados por el laboratorio.

La protección de los datos personales deberá aplicarse durante todo su ciclo de vida, desde su obtención hasta su eliminación, anonimización o destrucción definitiva.

---

2. Relación con la Política de Seguridad de la Información

La presente política deberá interpretarse conjuntamente con la Política de Seguridad y Gestión de la Información del Laboratorio DxMedica.

La Política de Protección de Datos Personales establece:

- Las finalidades para las cuales pueden utilizarse los datos.
- Los derechos de sus titulares.
- Las responsabilidades institucionales.

- Los principios aplicables al tratamiento.
- Las condiciones para comunicar datos a terceros.
- Las reglas de conservación y eliminación.

La Política de Seguridad y Gestión de la Información establece los controles técnicos y organizativos destinados a proteger dichos datos.

En caso de contradicción deberá aplicarse el criterio que otorgue mayor protección a la persona titular del dato, salvo que exista una obligación legal o sanitaria en sentido contrario.

---

3. Alcance

Esta política alcanza a:

- Pacientes.
- Representantes legales.
- Familiares y personas autorizadas.
- Médicos y profesionales derivantes.
- Personal del laboratorio.
- Autoridades.
- Patólogos.
- Técnicos.
- Personal administrativo.
- Equipo de Tecnología de la Información.
- Proveedores y contratistas.
- Instituciones sanitarias relacionadas.
- Estudiantes, investigadores o pasantes autorizados.
- Toda persona que acceda a información gestionada por el laboratorio.

La política se aplica a datos almacenados o tratados en:

- Bases de datos.
- Aplicaciones web.
- Portal de pacientes.
- Sistema de gestión del laboratorio.
- Sistema de gestión de pacientes.
- Sistema de trazabilidad.
- Sistema de carga desde quirófano.
- Integraciones y APIs.

- Servidores y contenedores.
- Copias de seguridad.
- Computadoras y dispositivos.
- Registros de auditoría.
- Documentación en papel.
- Imágenes.
- Fotografías.
- Códigos QR.
- Etiquetas.
- Vidrios.
- Casetes.
- Tacos.
- Muestras y otros soportes físicos relacionados con protocolos.

---

4. Marco normativo

El tratamiento de datos personales se realizará de acuerdo con:

- Ley 25.326 de Protección de los Datos Personales.
- Decreto 1558/2001, reglamentario de la Ley 25.326.
- Ley 26.529 de Derechos del Paciente, Historia Clínica y Consentimiento Informado.
- Normas complementarias y modificatorias.
- Disposiciones y resoluciones de la Agencia de Acceso a la Información Pública.
- Resolución AAIP 47/2018 sobre medidas de seguridad recomendadas para datos personales en medios informatizados y no informatizados.
- Normativa sanitaria nacional y provincial aplicable.
- Reglas profesionales y de habilitación aplicables a laboratorios de anatomía patológica.
- Obligaciones contractuales válidamente asumidas por el laboratorio.

La información relacionada con la salud es considerada un dato personal sensible y requiere medidas de protección reforzadas. Los establecimientos sanitarios y profesionales de la salud pueden tratar datos de sus pacientes respetando los principios de confidencialidad y secreto profesional.

---

5. Definiciones

5.1. Dato personal

Toda información referida a una persona identificada o que pueda ser identificada directa o indirectamente.

5.2. Dato sensible

Dato personal que revela información especialmente protegida, incluida la información relacionada con la salud física o mental, antecedentes médicos, diagnósticos, resultados, estudios genéticos o vida sexual.

5.3. Tratamiento

Cualquier operación realizada sobre datos personales, incluyendo:

- Recolección.
- Registro.
- Organización.
- Almacenamiento.
- Consulta.
- Modificación.
- Relacionamiento.
- Transmisión.
- Respaldo.
- Archivo.
- Eliminación.
- Destrucción.

5.4. Titular del dato

Persona a la que se refiere la información tratada.

5.5. Responsable

DXMedica, en cuanto determina las finalidades y formas generales en que se tratan los datos personales.

5.6. Usuario autorizado

Persona que accede a datos personales para cumplir funciones autorizadas por el laboratorio.

5.7. Seudonimización

Proceso mediante el cual los datos identificatorios se reemplazan por un código, manteniendo separada y protegida la información necesaria para relacionar el código con la identidad del paciente.

5.8. Anonimización o disociación

Proceso por el cual la información deja de poder asociarse razonablemente con una persona identificada o identificable.

5.9. Incidente de datos personales

Evento que produzca o pueda producir pérdida, alteración, destrucción, acceso, divulgación o utilización no autorizada de datos personales.

---

6. Responsable del tratamiento

El responsable institucional del tratamiento será:

DXMédica

Domicilio: **Avenida Alem 855, Bahía Blanca.**

Correo institucional para consultas sobre datos personales:
administración@dxmedica.ar

Teléfono institucional:
0291 451-1892

La autoridad institucional será el **Dr. Pablo Lespi**.

El referente operativo y tecnológico será **Ladislao Potocki**, sin perjuicio de las responsabilidades que correspondan a cada jefe de área y a cada usuario.

---

7. Principios aplicables

7.1. Licitud

Los datos serán tratados conforme a la normativa vigente, las finalidades informadas y las obligaciones sanitarias y profesionales del laboratorio.

7.2. Finalidad

Los datos solo podrán utilizarse para finalidades determinadas, explícitas, legítimas y relacionadas con la prestación de los servicios del laboratorio.

No podrán utilizarse posteriormente para finalidades incompatibles con las que motivaron su obtención.

7.3. Minimización

Solo se recopilarán los datos que resulten adecuados, pertinentes y necesarios.

No se solicitarán datos personales que no tengan una finalidad sanitaria, profesional, administrativa, legal, contractual, científica o de seguridad debidamente justificada.

7.4. Exactitud

Los datos deberán ser correctos, completos y actualizados cuando resulte necesario.

7.5. Confidencialidad

Toda persona que acceda a datos personales deberá mantener su confidencialidad, incluso después de finalizar su relación laboral, profesional o contractual con el laboratorio.

7.6. Seguridad

Se aplicarán medidas técnicas y organizativas para evitar pérdidas, adulteraciones, accesos no autorizados, divulgaciones y tratamientos indebidos.

7.7. Acceso restringido

Solo podrán acceder a los datos quienes los necesiten para cumplir sus funciones.

7.8. Conservación limitada

Los datos se conservarán durante el tiempo necesario para cumplir sus finalidades y los plazos legales, sanitarios, profesionales o contractuales aplicables.

7.9. Responsabilidad

Cada usuario será responsable por las acciones realizadas mediante su cuenta personal.

7.10. Trazabilidad

Las operaciones relevantes deberán quedar registradas para permitir la investigación de errores, incidentes y accesos indebidos.

---

8. Categorías de datos tratados

El laboratorio podrá tratar las siguientes categorías de datos:

8.1. Datos identificatorios

- Nombre y apellido.
- Documento de identidad.
- Fecha de nacimiento.
- Sexo consignado cuando resulte clínicamente necesario.
- Domicilio.
- Firma.
- Número interno de paciente.
- Código de protocolo.

8.2. Datos de contacto

- Teléfono.
- Correo electrónico.
- Domicilio.
- Datos de contacto de representantes o personas autorizadas.

8.3. Datos sanitarios

- Antecedentes clínicos.
- Diagnósticos presuntivos y definitivos.
- Información relacionada con cirugías y procedimientos.
- Datos de muestras.
- Informes anatomopatológicos.
- Resultados de biopsias y citologías.
- Estudios PAP.
- Información molecular o genética, cuando corresponda.
- Imágenes macroscópicas o microscópicas.
- Fotografías relacionadas con estudios.
- Descripciones macro y microscópicas.
- Interconsultas.
- Rectificaciones o ampliaciones de informes.

8.4. Datos de trazabilidad

- Origen de la muestra.
- Fecha y hora de recepción.
- Número de protocolo.
- Ubicación.
- Procesos realizados.
- Vidrios.

- Tacos.
- Casetes.
- Códigos QR.
- Profesionales intervinientes.
- Cambios de estado.

8.5. Datos administrativos y de facturación

- Obra social.
- Cobertura.
- Información de facturación.
- Institución derivante.
- Datos necesarios para autorizaciones y cobranzas.

8.6. Datos de profesionales

- Nombre.
- Matrícula.
- Especialidad.
- Institución.
- Datos de contacto.
- Estudios derivados.
- Actividad dentro de los sistemas.

8.7. Datos técnicos y de seguridad

- Usuario.
- Fecha y hora de acceso.
- Dirección IP.
- Equipo de origen.
- Acciones realizadas.
- Intentos fallidos de autenticación.
- Modificaciones de datos.
- Descargas de informes.
- Registros de auditoría.

8.8. Datos laborales

El laboratorio podrá tratar datos de empleados y colaboradores para la administración de las relaciones laborales, profesionales y contractuales.

---

9. Origen de los datos

Los datos podrán obtenerse de:

- El propio paciente.
- Su representante legal.
- Una persona debidamente autorizada.
- Médicos y profesionales derivantes.
- Clínicas, hospitales, consultorios o instituciones sanitarias.
- Obras sociales y financiadores.
- Solicitudes médicas.
- Muestras recibidas.
- Sistemas internos.
- Integraciones autorizadas.
- Registros generados por el uso de aplicaciones y portales.
- Fuentes habilitadas por una obligación legal o relación profesional.

El laboratorio deberá procurar identificar la fuente de los datos cuando estos no hayan sido proporcionados directamente por su titular.

---

10. Finalidades

Los datos personales podrán tratarse para:

- Identificar al paciente.
- Registrar solicitudes y protocolos.
- Recibir y procesar muestras.
- Realizar estudios anatomopatológicos.
- Elaborar, validar y emitir informes.
- Efectuar interconsultas.
- Garantizar la trazabilidad de muestras, tacos, vidrios y casetes.
- Comunicar la disponibilidad de resultados.
- Permitir el acceso al portal de pacientes.
- Entregar resultados a personas autorizadas.
- Coordinar cuestiones administrativas.
- Atender consultas.
- Cumplir obligaciones sanitarias y profesionales.
- Facturar y gestionar coberturas.
- Mantener registros clínicos.

- Garantizar la continuidad asistencial.
- Gestionar la calidad.
- Investigar errores e incidentes.
- Proteger los sistemas.
- Mantener copias de seguridad.
- Cumplir requerimientos judiciales o administrativos válidos.
- Realizar estadísticas, investigación o docencia cuando exista autorización o se hayan aplicado mecanismos adecuados de anonimización o disociación.

No se utilizarán datos de pacientes con fines publicitarios o comerciales ajenos a la prestación del servicio sin una autorización específica y válida.

---

11. Consentimiento y habilitación del tratamiento

Cuando la normativa exija consentimiento, este deberá ser:

- Libre.
- Previo.
- Expreso.
- Informado.
- Específico.
- Registrable o demostrable.

El consentimiento para una práctica médica no deberá confundirse con el consentimiento para tratamientos de datos que no sean necesarios para dicha práctica.

El tratamiento podrá realizarse sin solicitar un consentimiento adicional cuando los datos:

- Resulten necesarios para la relación profesional, sanitaria o contractual con el paciente.
- Sean necesarios para realizar el estudio solicitado.
- Deban tratarse para cumplir una obligación legal.
- Sean necesarios para proteger la salud o atender una emergencia en los casos legalmente previstos.
- Se encuentren debidamente anonimizados para fines científicos o estadísticos.
- Deban comunicarse en cumplimiento de una orden judicial válida.

El tratamiento de datos de salud deberá respetar siempre el secreto profesional.

---

12. Información al paciente

Al recopilar datos personales, el laboratorio deberá informar de manera clara:

- La identidad del responsable.
- La finalidad del tratamiento.
- Los datos solicitados.
- Cuáles datos son obligatorios.
- Las consecuencias de no proporcionarlos.
- Los posibles destinatarios.
- La existencia de sistemas y bases de datos.
- Los mecanismos para ejercer los derechos de acceso, rectificación y supresión.
- Los canales de contacto institucionales.

Esta información podrá proporcionarse mediante:

- Formularios.
- Cartelería.
- Portal web.
- Avisos de privacidad.
- Consentimientos.
- Comunicaciones institucionales.
- Solicitudes de estudio.

El aviso deberá ser comprensible y estar disponible antes o al momento de recopilar la información.

---

13. Seudonimización

El laboratorio utilizará como mecanismo principal de seudonimización un código asociado al protocolo.

El código podrá figurar en:

- Códigos QR.
- Etiquetas.
- Vidrios.
- Casetes.
- Tacos.
- Muestras.
- Imágenes.

- Documentación técnica.
- Sistemas de trazabilidad.
- Intercambios entre aplicaciones.

Siempre que sea posible, los elementos técnicos y de procesamiento mostrarán el código del protocolo en lugar de datos identificatorios completos.

La relación entre el código y el paciente deberá mantenerse en sistemas protegidos y solo será accesible para usuarios autorizados.

La información identificada mediante códigos continuará siendo considerada dato personal sensible mientras sea posible relacionarla con un paciente.

---

14. Anonimización

Cuando no sea necesario conservar la identidad del paciente, el laboratorio procurará anonimizar los datos.

La anonimización podrá aplicarse para:

- Estadísticas.
- Informes de gestión.
- Investigación.
- Capacitación.
- Control de calidad.
- Presentaciones académicas.
- Desarrollo o prueba de sistemas.

No se considerará anonimizada una información cuando exista una posibilidad razonable de identificar al paciente mediante el código de protocolo, las fechas, imágenes, características clínicas u otros datos combinados.

---

15. Acceso a la información

Todos los usuarios tendrán cuentas personales.

Los permisos se asignarán según:

- Área.
- Función.
- Rol profesional.
- Necesidad de acceso.

- Nivel de responsabilidad.

Queda prohibido:

- Compartir usuarios o contraseñas.
- Consultar datos por curiosidad.
- Acceder a pacientes sin una necesidad profesional o administrativa.
- Utilizar una cuenta ajena.
- Facilitar datos a personas no autorizadas.
- Descargar o copiar información sin finalidad laboral.
- Fotografiar pantallas, documentos o muestras con dispositivos personales sin autorización.

El acceso a datos de pacientes conocidos, familiares, compañeros de trabajo o personas públicas estará sujeto a las mismas reglas que cualquier otro acceso.

---

16. Altas, modificaciones y bajas

Las altas y modificaciones de usuarios deberán solicitarse mediante mensaje interno al área de Tecnología de la Información.

La solicitud deberá provenir del jefe o responsable del área correspondiente.

Ante una desvinculación, cambio de función o baja:

- El jefe del área deberá comunicar el hecho.
- La comunicación deberá realizarse preferentemente antes de que la baja se haga efectiva.
- El área de Tecnología de la Información deberá desactivar los accesos.
- Se deberán revocar sesiones, credenciales y permisos.
- Las cuentas se mantendrán deshabilitadas cuando sean necesarias para conservar la trazabilidad histórica.

---

17. Comunicación con pacientes

Las comunicaciones por WhatsApp, correo electrónico y teléfono se realizarán exclusivamente mediante números, cuentas y canales institucionales.

WhatsApp podrá utilizarse para:

Consultas administrativas.

- Información general.
- Avisos sobre disponibilidad de resultados.

- Indicaciones que no revelen información clínica sensible.

No se enviarán por WhatsApp:

- Informes anatomopatológicos.
- Diagnósticos.
- Resultados clínicos.
- Fotografías clínicas.
- Documentación sensible.
- Contraseñas.
- Credenciales de acceso.

Los informes deberán consultarse mediante el portal de pacientes, previa autenticación.

Antes de brindar información se deberá realizar una verificación razonable de identidad.

---

18. Entrega de informes

Los informes serán entregados o puestos a disposición mediante los sistemas y procedimientos autorizados.

El acceso deberá limitarse a:

- El paciente.
- Su representante legal.
- Una persona expresamente autorizada.
- El profesional derivante.
- La institución sanitaria legitimada para recibirlos.
- Otras personas habilitadas por la normativa aplicable.

Cuando el informe se encuentre disponible en el portal:

- El usuario deberá autenticarse.
- El acceso deberá realizarse mediante comunicación cifrada.
- Deberán registrarse los accesos relevantes.
- El informe no deberá ser accesible mediante una dirección pública sin autenticación.

No se brindará información clínica detallada por teléfono cuando no resulte posible verificar adecuadamente la identidad del interlocutor.

---

19. Cesión y comunicación a terceros

Los datos solo podrán comunicarse a terceros cuando:

- Sea necesario para la finalidad asistencial o diagnóstica.
- Exista consentimiento válido.
- Exista una relación profesional o contractual que lo justifique.
- Exista una obligación legal.
- Medie una orden judicial válida.
- Sea necesario para una interconsulta.
- Los datos hayan sido adecuadamente anonimizados.
- Se presente una emergencia o supuesto permitido por la normativa.

Los destinatarios podrán incluir:

- Médicos derivantes.
- Instituciones sanitarias.
- Laboratorios de referencia.
- Obras sociales.
- Proveedores tecnológicos.
- Servicios de alojamiento o respaldo.
- Proveedores de mantenimiento.
- Plataformas de integración.
- Autoridades competentes.

Solo se comunicarán los datos mínimos necesarios.

Los terceros deberán estar sujetos a obligaciones de confidencialidad, seguridad y uso limitado de la información.

---

20. Proveedores y encargados

Antes de contratar un proveedor que acceda a datos personales deberá evaluarse:

- Qué datos necesita.
- Para qué finalidad.
- Cómo accederá.
- Dónde almacenará la información.
- Qué medidas de seguridad utiliza.
- Qué personal podrá acceder.
- Si existen subcontratistas.

- Cómo informa incidentes.
- Cómo devuelve o elimina la información al finalizar el servicio.
- Si procesa información fuera de Argentina.

Los contratos deberán incluir, cuando corresponda:

- Deber de confidencialidad.
- Limitación de finalidad.
- Medidas de seguridad.
- Comunicación de incidentes.
- Prohibición de utilización propia.
- Reglas de subcontratación.
- Devolución o eliminación de datos.
- Auditorías o evidencias de cumplimiento.

---

21. Integración con APIs

Las integraciones, deberán transmitir únicamente los datos necesarios para su finalidad.

Antes de habilitar una integración se deberá determinar:

- Qué datos se envían.
- Si contienen identificadores del paciente.
- Si pueden utilizarse códigos de protocolo.
- Quién recibe la información.
- En qué país se procesa.
- Durante cuánto tiempo se conserva.
- Qué sistema de autenticación se utiliza.
- Si la comunicación se encuentra cifrada.
- Cómo se registran los envíos.
- Qué ocurre ante errores o indisponibilidad.

Las credenciales de las APIs deberán almacenarse de forma protegida y no podrán incluirse en código fuente público ni compartirse por canales no autorizados.

---

22. Transferencias internacionales

Antes de transferir datos personales fuera de Argentina deberá verificarse:

- El país de destino.

- El nivel de protección aplicable.
- La finalidad de la transferencia.
- La necesidad de enviar datos identificatorios.
- La existencia de consentimiento o habilitación legal.
- Los contratos y garantías aplicables.
- La posibilidad de anonimizar o seudonimizar la información.

Cuando el país de destino no posea un nivel de protección reconocido como adecuado, deberán aplicarse las garantías contractuales o mecanismos permitidos por la normativa argentina.

---

23. Seguridad de los datos

DXMédica aplicará las medidas previstas en su Política de Seguridad y Gestión de la Información.

Entre las medidas actuales se incluyen:

- Servidor dedicado.
- Aplicaciones y servicios en contenedores aislados.
- Separación de bases de datos y aplicaciones.
- Acceso administrativo mediante SSH.
- Puerto de acceso no estándar.
- Firewall con acceso limitado a direcciones IP autorizadas.
- Cuentas personales.
- Registro de cambios.
- Red aislada para equipos personales.
- Utilización preferente de conexiones cableadas para equipos del laboratorio.
- Portal de pacientes con autenticación.
- Copias de seguridad externas cifradas.
- Copias completas semanales.
- Copias incrementales diarias.
- Respaldo horario de registros binarios de bases de datos.
- Pruebas de restauración semestrales.

Las medidas deberán revisarse periódicamente y adaptarse a los riesgos existentes. La AAIP recomienda la aplicación de medidas administrativas, técnicas, físicas y de mejora continua para datos informatizados y no informatizados.

---

24. Copias de seguridad

Las copias de seguridad podrán contener datos personales y deberán recibir el mismo nivel de protección que los sistemas originales.

El esquema de respaldo incluirá:

- Copias completas semanales.
- Copias incrementales diarias.
- Copias horarias de registros binarios.
- Almacenamiento en un servidor externo.
- Cifrado de los respaldos.
- Acceso limitado a personal autorizado.
- Prueba de restauración, como mínimo, cada seis meses.

Se conservarán:

- Las últimas cuatro copias completas.
- Las copias incrementales necesarias para restaurar los ciclos conservados.
- Los registros binarios necesarios para la recuperación prevista.

La eliminación de backups deberá realizarse mediante procedimientos que impidan su recuperación no autorizada.

---

25. Registros de auditoría

Los sistemas deberán mantener registros de acciones relevantes, incluyendo, cuando sea posible:

- Usuario.
- Fecha y hora.
- Dirección IP.
- Sistema utilizado.
- Datos consultados.
- Registro afectado.
- Cambios realizados.
- Valor anterior y posterior.
- Descargas.
- Validaciones.
- Intentos fallidos.
- Altas y bajas de usuarios.

Los logs:

- Serán confidenciales.
- Tendrán acceso restringido.
- No podrán modificarse sin autorización.
- Podrán consultarse para auditorías, incidentes, control de calidad y seguridad.
- No podrán utilizarse para finalidades incompatibles o vigilancia indiscriminada.

---

26. Conservación de información

Los datos se conservarán durante los plazos establecidos por:

- Normas sanitarias.
- Normas de protección de datos.
- Obligaciones profesionales.
- Necesidades asistenciales.
- Requisitos médico-legales.
- Contratos aplicables.
- Políticas institucionales documentadas.

La supresión no procederá cuando exista una obligación de conservación o cuando pueda afectar derechos legítimos del paciente, del laboratorio o de terceros.

26.1. Tacos y vidrios

Los tacos y vidrios correspondientes a biopsias y citologías, con excepción de los estudios PAP, se conservarán durante un plazo mínimo de diez años.

Finalizado dicho plazo, el área de Patólogos decidirá si:

- Se mantienen.
- Se seleccionan para conservación prolongada.
- Se destruyen.

El área de Patólogos determinará el procedimiento apropiado y deberá dejar constancia de la decisión.

Los estudios PAP se conservarán conforme al plazo específico que establezcan la normativa y el procedimiento interno correspondiente.

26.2. Información digital

Los informes, protocolos, registros de trazabilidad, consentimientos e información clínica digital deberán conservarse durante los plazos legal y profesionalmente aplicables.

26.3. Documentación en papel

La eliminación de documentación en papel solo podrá realizarse cuando:

- El registro digital sea completo.
- Sea legible.
- Esté correctamente asociado al protocolo.
- Se encuentre respaldado.
- Se garantice su integridad.
- Haya vencido el plazo de conservación del original o esté permitida su sustitución.
- Exista autorización.

---

27. Digitalización

DXMédica promoverá la sustitución progresiva de registros en papel por sistemas digitales que permitan identificar y trazar muestras, preparados, vidrios, casetes, tacos y demás elementos mediante códigos QR u otros identificadores únicos.

La digitalización deberá garantizar:

- Integridad.
- Autenticidad.
- Legibilidad.
- Perdurabilidad.
- Trazabilidad.
- Recuperabilidad.
- Acceso restringido.
- Registro de modificaciones.

La historia clínica informatizada debe contar con mecanismos que aseguren su integridad, autenticidad, inalterabilidad y recuperación.

---

28. Derechos de las personas

Los titulares podrán ejercer sus derechos de:

- Información.
- Acceso.
- Rectificación.
- Actualización.
- Supresión, cuando corresponda.

- Confidencialidad.

28.1. Derecho de acceso

La persona podrá solicitar información sobre:

- Los datos almacenados.
- Su origen.
- Las finalidades.
- Los destinatarios.
- Las comunicaciones realizadas.
- Los mecanismos de tratamiento.

La respuesta deberá proporcionarse dentro de los diez días corridos desde la recepción de una solicitud fehaciente y debidamente acreditada.

28.2. Rectificación y actualización

Los datos inexactos o incompletos deberán rectificarse o actualizarse dentro de los cinco días hábiles desde la recepción del reclamo o desde que se advierta el error.

Las correcciones de información clínica deberán mantener la trazabilidad y no podrán eliminar indebidamente el registro original.

28.3. Supresión

La persona podrá solicitar la supresión cuando los datos:

- Se hayan obtenido de forma ilegítima.
- Sean innecesarios.
- Se utilicen para finalidades incompatibles.
- Hayan vencido sus plazos de conservación.

La supresión no procederá cuando:

- Exista una obligación legal o sanitaria de conservación.
- Sea necesario mantener la historia clínica.
- Puedan afectarse derechos legítimos de terceros.
- Los datos sean necesarios para ejercer o defender derechos.
- La información deba conservarse por razones médico-legales.

28.4. Documentación clínica

Cuando corresponda una solicitud de copia de historia clínica o documentación clínica alcanzada por la Ley 26.529, se aplicarán los procedimientos y plazos especiales previstos

en dicha norma. La ley establece la entrega de copia dentro de las cuarenta y ocho horas desde su solicitud, salvo situaciones de emergencia.

---

29. Procedimiento para ejercer derechos

Las solicitudes deberán dirigirse a:

Correo electrónico: **administracion@dxmedica.ar**

Domicilio: **Avenida Alem 855, Bahía Blanca**

La solicitud deberá indicar:

- Nombre y apellido.
- Documento.
- Datos de contacto.
- Derecho que desea ejercer.
- Información o protocolo relacionado.
- Documentación que acredite identidad o representación.

El laboratorio deberá verificar la identidad antes de entregar o modificar datos.

Cuando la solicitud sea realizada por otra persona, deberá acreditarse:

- Representación legal.
- Autorización.
- Vínculo y habilitación legal.
- Condición de sucesor, cuando corresponda.

Las solicitudes y respuestas deberán quedar registradas.

---

30. Datos de niños, niñas y adolescentes

Los datos de personas menores de edad deberán recibir protección reforzada.

El acceso, consentimiento y entrega de información se gestionarán conforme a:

- Edad.
- Grado de madurez.
- Representación legal.
- Interés superior del menor.
- Autonomía progresiva.
- Normativa sanitaria aplicable.

No se entregará información automáticamente a cualquier adulto que la solicite. Deberá verificarse su identidad, representación y legitimación.

---

31. Personas fallecidas

Las solicitudes relacionadas con personas fallecidas serán evaluadas conforme a la normativa aplicable.

Quien solicite información deberá acreditar:

- Identidad.
- Vínculo.
- Condición de sucesor o representante.
- Finalidad legítima.

La información de terceros que figure en la documentación deberá protegerse.

---

32. Investigación, docencia y estadísticas

El uso de datos para investigación, docencia, publicaciones o presentaciones deberá:

- Tener una finalidad legítima.
- Contar con las autorizaciones correspondientes.
- Limitar los datos utilizados.
- Priorizar la anonimización.
- Evitar imágenes o combinaciones de datos que permitan identificar al paciente.
- Respetar los requisitos éticos y legales.

Las exposiciones académicas que puedan identificar a un paciente requerirán las autorizaciones aplicables.

---

33. Incidentes

Todo incidente que afecte datos personales deberá comunicarse inmediatamente a:

- Dr. Pablo Lespi.
- Ladislao Potocki.

Se consideran incidentes, entre otros:

- Acceso no autorizado.

- Envío de información al destinatario equivocado.
- Pérdida de documentos.
- Pérdida de dispositivos.
- Robo de credenciales.
- Malware o ransomware.
- Exposición en Internet.
- Modificación de informes.
- Eliminación accidental.
- Falla de backups.
- Pérdida de trazabilidad.
- Acceso injustificado de un empleado.
- Exposición de credenciales de API.

La respuesta deberá incluir:

1. Contención.
2. Preservación de evidencias.
3. Identificación de datos afectados.
4. Evaluación de personas afectadas.
5. Recuperación de los sistemas.
6. Documentación.
7. Acciones correctivas.
8. Evaluación de comunicaciones legales o contractuales.

El personal no deberá ocultar incidentes.

---

34. Registro de bases de datos

El laboratorio deberá verificar qué bases de datos se encuentran alcanzadas por las obligaciones de inscripción ante el Registro Nacional de Bases de Datos Personales y mantener actualizada la información correspondiente.

La inscripción deberá reflejar, cuando resulte aplicable:

- Responsable.
- Domicilio.
- Finalidad.
- Categorías de datos.
- Origen.
- Destinatarios.

- Medidas de seguridad.
- Personas con acceso.
- Plazos de conservación.
- Procedimientos para ejercer derechos.

La AAIP informa que las bases alcanzadas deben encontrarse inscriptas y mantener actualizada su información.

---

35. Confidencialidad del personal

Toda persona con acceso deberá firmar o aceptar compromisos de confidencialidad acordes con sus funciones.

La obligación subsistirá después de:

- La baja laboral.
- El cambio de puesto.
- La finalización de una contratación.
- La finalización de una práctica profesional o académica.

La información no podrá utilizarse en beneficio propio o de terceros.

---

36. Capacitación

El personal deberá recibir capacitación periódica sobre:

- Protección de datos personales.
- Datos sensibles.
- Secreto profesional.
- Uso seguro de sistemas.
- Contraseñas.
- Phishing y fraude.
- Comunicación con pacientes.
- Uso institucional de WhatsApp y correo.
- Notificación de incidentes.
- Gestión de documentación.
- Seudonimización.
- Derechos de los pacientes.

La capacitación deberá adecuarse a las funciones de cada área.

37. Incumplimientos

El incumplimiento podrá dar lugar a:

- Restricción de accesos.
- Suspensión de cuentas.
- Revisión de permisos.
- Capacitación obligatoria.
- Medidas disciplinarias.
- Medidas contractuales.
- Comunicación a las autoridades.
- Acciones legales cuando correspondan.

Las medidas deberán aplicarse de acuerdo con la gravedad, intencionalidad, reiteración y consecuencias del incumplimiento.

---

38. Excepciones

Toda excepción deberá:

- Estar justificada.
- Ser autorizada por la autoridad correspondiente.
- Identificar los datos afectados.
- Determinar su duración.
- Establecer medidas compensatorias.
- Quedar documentada.

No podrán autorizarse excepciones que contradigan obligaciones legales.

---

39. Procedimientos complementarios

Esta política deberá complementarse con:

1. Aviso de privacidad para pacientes.
2. Procedimiento de ejercicio de derechos.
3. Procedimiento de alta y baja de usuarios.
4. Compromiso de confidencialidad.
5. Procedimiento de entrega de informes.
6. Procedimiento de comunicación por WhatsApp, correo y teléfono.

7. Procedimiento de gestión de incidentes.
8. Procedimiento de copias de seguridad y restauración.
9. Procedimiento de digitalización y destrucción.
10. Procedimiento de conservación de tacos y vidrios.
11. Registro de proveedores con acceso a datos.
12. Inventario de bases de datos.
13. Registro de actividades de tratamiento.
14. Procedimiento de investigación y docencia.
15. Política de Seguridad y Gestión de la Información.

---

40. Revisión

La política será revisada como mínimo una vez al año.

También deberá revisarse ante:

- Cambios normativos.
- Incidentes relevantes.
- Nuevos sistemas.
- Nuevas integraciones.
- Incorporación del inicio de sesión centralizado.
- Incorporación de doble factor.
- Cambios en los plazos de conservación.
- Cambios en autoridades o responsables.
- Observaciones de auditoría.
