 UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES
Andes 1365 piso 7, 11100, Montevideo, Uruguay
+598 2901 00 65 opción 3
www.datospersonales.gub.uy



3 { **PROTECCIÓN DE
DATOS EN SALUD**



PROTECCIÓN DE DATOS DE SALUD

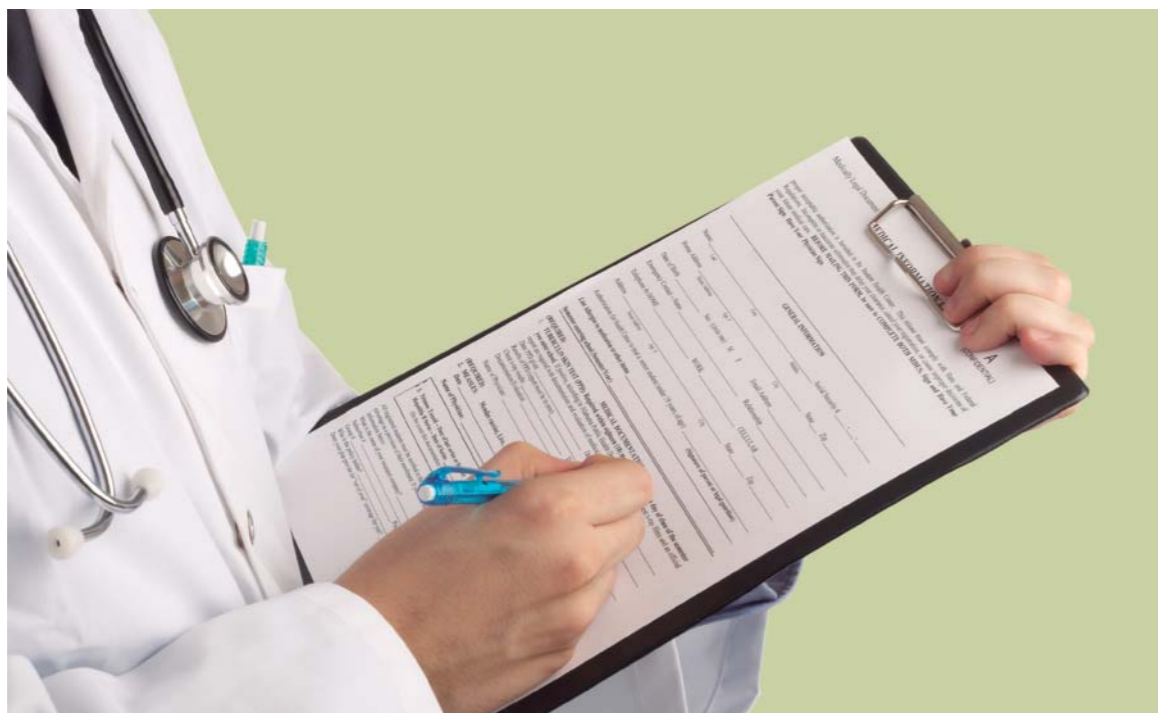
¿Por qué merecen una protección especial?

Hay ciertos datos personales que describen los aspectos más sensibles o delicados sobre el individuo y que pertenecen a la esfera más intangible de la persona, como su estado de salud, sus características físicas, ideología o vida sexual entre otros. Por esta razón, solo pueden ser objeto de tratamiento con el consentimiento expreso y escrito de su titular.

Los datos relativos a la salud física o mental de los pacientes pueden ser recolectados y tratados por establecimientos sanitarios públicos o privados y por profesionales vinculados a la salud, siempre y cuando se respeten los principios del secreto profesional y las disposiciones en materia de protección de datos, o por razones de interés general autorizadas por Ley.

Dentro de la historia clínica de cada usuario del sistema de salud, se encuentran datos que son parte de su esfera íntima y refieren a enfermedades pasadas, presentes, tratamientos recibidos, adicciones -si las tiene- e información genética, entre otros. Puede además contener otros datos sensibles tales como raza, vida sexual o creencias religiosas.

Los datos de salud y la historia clínica tienen un rol primordial en nuestras vidas y de ellos depende en gran medida la asistencia sanitaria que recibimos, que se fundamenta en la información correcta sobre el paciente con la que cuentan los médicos y los centros asistenciales. La posibilidad de contar con una historia clínica completa es un derecho de los pacientes.



DERECHOS Y OBLIGACIONES ESPECÍFICAS A LA SALUD

Con la excepción de situaciones de emergencia, los datos deberán recabarse directamente del paciente para garantizar su veracidad.

Se debe obtener consentimiento informado y por escrito en forma libre, previa y expresa para el tratamiento de datos. Además se requiere que se informe al paciente -en lenguaje comprensible- todas las incidencias posibles, salvo que existan razones de urgencia o emergencia, notoria fuerza mayor, riesgo grave para la salud del paciente, o riesgo cierto para la sociedad.

El centro asistencial deberá llevar una historia clínica completa, escrita o electrónica, donde figure la evolución del estado de salud desde el nacimiento hasta la muerte. En casos donde el usuario cambia de institución o sistema de cobertura asistencial, se recabará la historia clínica completa de origen.

La historia clínica registrará los procedimientos médicos de urgencia o emergencia, o de notoria fuerza mayor además de los comunes.

Se podrá obtener una copia de la misma y ejercer los derechos de rectificación, actualización, inclusión o supresión de datos. En el caso de personas fallecidas, el ejercicio del derecho de acceso corresponderá a cualquiera de sus sucesores universales, que acrediten debidamente esta calidad.

Se publicará la nómina de profesionales que se desempeñan en el servicio de salud, sus nombres, especialidades y demás datos disponibles, así como sus días y horarios de consulta. Asimismo, existe el derecho a conocer los nombres, cargos y funciones de cualquier trabajador de la salud que participe en la atención del paciente.

Las instituciones presentarán sus bases de datos personales ante la Unidad Reguladora y de Control de Datos Personales, para que sean registradas, de acuerdo con la normativa vigente.



Cláusulas de consentimiento

En la página Web de la URCDP www.datospersonales.gub.uy se pone a disposición de médicos e instituciones médicas, modelos de cláusulas de consentimiento para facilitar la recopilación de información clínica completa y veraz, cumpliendo con los requisitos legales expresados en la normativa.

¿Cómo deben resguardarse los datos de salud?

Los centros asistenciales están obligados a implementar medidas de seguridad respecto a las historias clínicas, tanto escritas como electrónicas.

Las mismas tienen carácter reservado y a ellas pueden acceder únicamente los responsables de la atención médica y el personal administrativo vinculado; el paciente, en algunos casos la familia y el Ministerio de Salud Pública.

Sería recomendable que los centros de salud contaran con una política y un documento que describa los procedimientos relativos a la seguridad de información, así como un responsable de seguridad que desarrolle programas de difusión y sensibilización del personal sobre las medidas dispuestas en las políticas de seguridad.

En el caso de traslado de información o documentos se deberán tomar las medidas necesarias para mantener su integridad. Asimismo, la destrucción de la información no debe permitir su recuperación posterior.

Todos estos aspectos deben garantizarse también cuando el tratamiento de datos sea realizado por un tercero a cuenta del centro asistencial, por ejemplo a través de cláusulas contractuales y supervisando la tarea.

El rol de la Unidad Reguladora y de Control de Datos Personales (URCDP)

En caso de que surjan dudas respecto al tratamiento que debe darse a los datos de salud, se puede acudir ante la Unidad Reguladora y de Control de Datos Personales, a efectos de que emita opinión sobre la cuestión planteada.

La Unidad es competente además para resolver ante las denuncias recibidas, determinando si existió contravención a la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data.

De existir una contravención a la Ley la Unidad puede imponer las sanciones que corresponda.

