SUPERINTENDENCIA DE SERVICIOS DE SALUD

Disposición 2/2021

DI-2021-2-APN-GG#SSS

Ciudad de Buenos Aires, 02/02/2021

VISTO el Expediente Nº EX-2020-59712532-APN-GG#SSS, las Leyes Nº 23.660, Nº 23.661, Nº 23.798, N° 25.326, N° 26.529, N° 27.275, los Decretos N° 1244 de fecha 1º de julio de 1991, N° 1615 de fecha 23 de diciembre de 1996 y Nº 2710 de fecha 28 de diciembre de 2012, las Resoluciones Nº 220 de fecha 10 de mayo de 2006, Nº 695 de fecha 13 de agosto de 2008, Nº 1006 de fecha 16 de noviembre de 2017, Nº 642 de fecha 20 de julio de 2018 y Nº 123 de fecha 14 de enero de 2021, todas de la SUPERINTENDENCIA DE SERVICIOS DE SALUD, la Disposición Nº 1 de fecha 19 de febrero de 2015 de la Oficina Nacional de Tecnologías de Información, y

CONSIDERANDO:

Que por Decreto N° 1615/96 se ordenó la fusión de la ADMINISTRACIÓN NACIONAL DEL SEGURO DE SALUD (ANSSAL), el INSTITUTO NACIONAL DE OBRAS SOCIALES (INOS) y la DIRECCIÓN NACIONAL DE OBRAS SOCIALES (DINOS), constituyendo la SUPERINTENDENCIA DE SERVICIOS DE SALUD como organismo descentralizado de la Administración Pública Nacional y en jurisdicción del MINISTERIO DE SALUD.

Que mediante el Decreto Nº 2710/12 se aprobó la estructura organizativa de la SUPERINTENDENCIA DE SERVICIOS DE SALUD, cuyo Anexo II define sus objetivos, entre los que se encuentra “efectuar el contralor del cumplimiento de las obligaciones éticas correspondientes al organismo y a todos sus dependientes y desarrollar mecanismos de control y procesos contra fraude y corrupción”.

Que por Resolución Nº 220/2006 esta SUPERINTENDENCIA DE SERVICIOS DE SALUD creó el Comité de Seguridad de la Información, integrado por los Gerentes de todas las áreas sustantivas del Organismo, a los efectos de proyectar y delinear las propuestas para conformar el modelo de política de seguridad de la información a adoptar.

Que mediante la Resolución del Registro de la SUPERINTENDENCIA DE SERVICIOS DE SALUD Nº 695/2008 se aprobaron los lineamientos básicos propuestos por el citado Comité para integrar el Modelo de Política de Seguridad de la Información a adoptar por este Organismo, así como el Reglamento de Funcionamiento del Comité de Seguridad de la Información y la Política de Privacidad para entidades usuarias del sitio web.

Que por Disposición del Registro de la Oficina Nacional de Tecnologías de Información (ONTI) Nº 1/2015 se aprobó la Política de Seguridad de la Información Modelo, actualmente vigente.

Que, por Resolución Nº 642/18 de la SUPERINTENDENCIA DE SERVICIOS DE SALUD, se aprobó el Reglamento de Funcionamiento del Comité de Seguridad de la Información del Organismo, los Principios Básicos del Modelo de

Política de Seguridad de la Información, la Política de Control de Acceso a la Información en Formato Papel y la Política de Control de Acceso a la Información Web.

Que el Anexo II del mencionado reglamento de funcionamiento del Comité de Seguridad de la Información determinó que la clasificación de la información corresponde que sea realizada por cada Unidad Organizativa del Organismo, según el caso, en pública, reservada de uso interno, reservada confidencial y reservada secreta, aplicando -de corresponder- la Ley de Protección de Datos Personales.

Que el Comité de Seguridad de la Información celebró su asamblea anual ordinaria con fecha 4 de diciembre de 2019, en la que se decidió dar comienzo con el proceso de clasificación de la información del Organismo durante el año 2020.

Que, en este sentido, oportunamente el Sr. Gerente General instruyó instrumentar las acciones necesarias, a través del citado Comité, para la clasificación de la información por áreas, a los efectos de contar con una herramienta que permita la resolución de los trámites en un marco jurídico que resguarde la información, asignando el tratamiento adecuado, según corresponda.

Que por la Resolución Nº 123/21 de la SUPERINTENDENCIA DE SERVICIOS DE SALUD se aprobó el Protocolo de excepción para el recupero por prestaciones a beneficiarios con Infección por VIH, en función del cual los Agentes del Seguro de Salud deberán presentar, de manera exclusiva a través de la plataforma de TRÁMITES A DISTANCIA (TAD), para cada período cuatrimestral allí previsto, una planilla con el detalle de los beneficiarios con infección por HIV a los que brindaron las prestaciones señaladas, sobre la base de módulos predefinidos.

Que a los efectos de otorgar el debido tratamiento a dichas planillas en el marco de la plataforma señalada y en su vinculación con el sistema de Gestión Electrónica de Documentos Oficiales (GEDO), la GERENCIA DE GESTIÓN ESTRATÉGICA ha requerido que se clasifique la información contenida en las planillas a presentar, las que necesariamente contendrán datos personales e información sensible referente a la salud de los beneficiarios involucrados.

Que, asimismo, los datos incluidos en dichas actuaciones serán entregados por los Agentes del Seguro de Salud a la SUPERINTENDENCIA DE SERVICIOS DE SALUD, en virtud de la posición de ente regulador del organismo, con el fin específico de tramitar los recuperos económicos que la normativa autoriza, asegurando los derechos de los beneficiarios.

Que los datos que recibirá el organismo se encuentran resguardados por los profesionales de la salud bajo el secreto médico.

Que la Ley Nº 25.326 tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, entendiendo por datos personales la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables, y como datos sensibles los que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Que, en su artículo 8°, la Ley de Protección de los Datos Personales indica con respecto a los datos relativos a la salud que “Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional”.

Que esta Ley consagra los principios de finalidad, confidencialidad y excepciones de entrega al mencionar que “los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención” (artículo 4º); “1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública” (artículo 10); y “la información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a (...) el desarrollo de funciones de control de la salud y del medio ambiente…” (artículo 17).

Que, asimismo, estos principios hallan su correlato en lo previsto en el artículo 38 del Decreto Nº 1759/72 (t.o. 2017), al establecer que “la parte interesada, su apoderado o letrado patrocinante, podrán tomar vista del expediente durante todo su trámite, con excepción de actuaciones, diligencias, informes o dictámenes que a pedido del órgano competente y previo asesoramiento del servicio jurídico correspondiente, fueren declarados reservados o secretos mediante decisión fundada del respectivo Subsecretario del Ministerio o del titular del ente descentralizado de que se trate”.

Que la Ley N° 26.529, de derechos del paciente en su relación con los Profesionales e Instituciones de la Salud, enuncia en su artículo 2º los derechos a la intimidad, donde toda actividad médico-asistencial tendiente a obtener, clasificar, utilizar, administrar, custodiar y transmitir información y documentación clínica del paciente debe observar el estricto respeto por la dignidad humana y la autonomía de la voluntad, así como el debido resguardo de su intimidad y la confidencialidad de sus datos sensibles; y a la confidencialidad, en función del cual el paciente tiene derecho a que toda persona que participe en la elaboración o manipulación de la documentación clínica, o bien tenga acceso a su contenido, guarde la debida reserva, salvo expresa disposición en contrario emanada de autoridad judicial competente o autorización del propio paciente.

Que, por su parte, la Ley N° 27.275 tiene por objeto garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública.

Que esta Ley establece un límite al ejercicio del derecho de Acceso a la Información Pública, afirmando que los sujetos obligados podrán exceptuarse de proveer la información (artículo 8º) cuando comprometa los derechos o intereses legítimos de un tercero obtenida en carácter confidencial,esté protegida por el secreto profesional y cuando contenga datos personales y no pueda brindarse aplicando procedimientos de disociación, salvo que se cumpla con las condiciones de licitud previstas en la Ley Nº 25.326, de protección de datos personales y sus modificatorias.

Que, a la luz de la normativa mencionada y la sensibilidad de los datos que forman parte de las actuaciones, corresponde resguardarlas del acceso por parte de terceros ajenos a su trámite.

Que, en este entendimiento, la GERENCIA DE GESTIÓN ESTRATÉGICA sostuvo que las actuaciones cuya clasificación propone contienen datos personales y sensibles, cuyo resguardo es obligatorio, y que corresponde tratarlos conforme su carácter “RESERVADA - CONFIDENCIAL”, por cuanto se trata de “Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros”, conforme se describe en la Disposición Nº 1/15-ONTI.

Que correlativamente a la clasificación señalada, y para garantizar la protección de la información en el sistema de Gestión Electrónica de Documentos Oficiales (GEDO), conforme resulta del requerimiento de la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS, debe otorgársele carácter de INFORME RESERVADO (IFRE) en dicho sistema.

Que, del mismo modo, deberá estar habilitado con el permiso denominado “GEDO CONFIDENCIAL” para la repartición y personas a las que corresponda tratar el documento.

Que al tratarse de un trámite que deberá llevar adelante en la GERENCIA DE GESTIÓN ESTRATÉGICA y cuyos responsables podrían variar durante el transcurso de su ejecución, corresponde autorizar a su autoridad máxima a definir los usuarios asignados para la visualización y tratamiento de la información.

Que la GERENCIA GENERAL de la SUPERINTENDENCIA DE SERVICIOS DE SALUD tiene asignada la responsabilidad primaria por la garantía de la seguridad de la información del organismo, mientras que el Sr. Gerente de Gestión Estratégica tiene a su cargo la coordinación del Comité de Seguridad de la Información, coincidiendo en la procedencia de la propuesta de clasificación de la información formulada, y han concluido que los datos personales y sensibles que se pretende reservar pertenecen a los beneficiarios de Agentes del Seguro de Salud y son entregados al organismo con la confianza de que serán resguardados y utilizados solamente para el fin específico de obtener el reintegro económico de las prestaciones brindadas.

Que la clasificación que se propone no afecta en modo alguno a la transparencia en la gestión pública y el control ciudadano de los actos de la administración, que resulta ejercido por las propias partes intervinientes en los procedimientos que se sustancian en tales actuaciones.

Que las Gerencias de Gestión Estratégica y de Asuntos Jurídicos han tomado la intervención de sus respectivas competencias.

Que la presente se dicta en uso de las facultades conferidas por los Decretos Nº 1615/96, Nº 2710/12 y Nº 599/20.

Por ello

EL GERENTE GENERAL DE LA SUPERINTENDENCIA DE SERVICIOS DE SALUD

DISPONE:

ARTÍCULO 1º.- Declárase sensibles los datos personales contenidos en las planillas con el detalle de los beneficiarios con infección por HIV que recibieron prestaciones por parte de los Agentes del Seguro de Salud, que éstos deben presentar en función de lo previsto en los Anexos I (IF-2021-02623042-APN-SGE#SSS) y II (IF-2021-03227234-APN-SGE#SSS) de la Resolución Nº 123/21 de la SUPERINTENDENCIA DE SERVICIOS DE SALUD, y/o la normativa que en el futuro la sustituya.

ARTÍCULO 2°.- Declárase “RESERVADA – CONFIDENCIAL” toda información contenida en las actuaciones referidas en el artículo anterior.

ARTÍCULO 3º.- Instrúyese al titular de la GERENCIA DE GESTIÓN ESTRATÉGICA para que designe e informe a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS los agentes de dicha Gerencia que tendrán acceso a los documentos alcanzados, así como también las eventuales modificaciones que se fueren sucediendo.

ARTÍCULO 4°.- Requiérase a la SECRETARÍA DE INNOVACIÓN PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS que habilite para inicio y firma el documento “INFORME RESERVADO” (IFRE) con la información señalada en el artículo 1º a la repartición “Subgerencia de Gestión Estratégica (SGE#SSS)”, responsable de su tramitación.

ARTÍCULO 5º.- Regístrese, comuníquese, publíquese, dese a la DIRECCIÓN NACIONAL DEL REGISTRO OFICIAL y, oportunamente, archívese.

David Aruachan

e. 04/02/2021 N° 5011/21 v. 04/02/2021

Fecha de publicación 04/02/2021