NOVARTIS

Standard Operating Procedure (SOP) para el Tratamiento de Datos Personales

Country: Colombia

Division: All

Version No.: 4.0

Issue Date: May 1, 2022.

Effective Date: April 30, 2025.

Autor:	**Firma:**
Beatriz Quintana Escudero Head Data Privacy Arg. & South America	Quintana Escudero Beatriz Digitally signed by Quintana Escudero Beatriz DN: dc=com, dc=novartis, ou=people, ou=PH, serialNumber=3005014, cn=Quintana Escudero Beatriz Reason: I am the author of this document Date: 2022.04.29 12:24:22 -03'00'
Autorizó:	
Ximena Forero Cluster Legal Head	Forero Velasquez Ximena Margarita Digitally signed by Forero Velasquez Ximena Margarita DN: dc=com, dc=novartis, ou=people, ou=PH, serialNumber=634601, cn=Forero Velasquez Ximena Margarita Reason: I am approving this document Date: 2022.04.30 11:07:31 -05'00'

Contenido

1. Reemplazo

El presente SOP reemplaza el Standard Operating Procedure para el Manejo y Protección de Información Personal, versión 3.

2. Propósito

Las empresas del Grupo Novartis son organizaciones basadas en el conocimiento donde la información es un activo valioso.

Para cumplir con sus objetivos, Novartis utiliza datos personales de sus colaboradores, profesionales de la salud, investigadores, pacientes y otros terceros.

Novartis respeta los derechos a la protección de datos y de privacidad de toda persona que nos confíe sus datos personales, respetando las leyes y normativas que protegen dicha información, así como los estándares internacionales.

El objetivo del presente es dejar constancia de que se ha decidido que en el futuro la organización se regirá por la Política Global de Privacidad de Novartis (actualmente, versión 3.1).

Adicionalmente, y atendiendo a los requerimientos que sobre esta materia establece la normativa colombiana sobre protección de datos personales, se implementan procedimientos específicos para este país. Consecuentemente, el presente SOP describe los procedimientos específicos que deben aplicarse en la organización, los cuales son complementarios de aquellos previstos en la política global.

3. Alcance

Este SOP aplica a todas las compañías de Novartis en la República de Colombia (referidas en adelante como la "Compañía") y todos los colaboradores de la Compañía, así como los terceros que, actuando por cuenta y orden de la Compañía incluyendo contratistas, procesen datos personales que se encuentre almacenada en cualquier tipo de formato (sistemas, archivos electrónicos, bases de datos, documentos físicos impresos, escritos, imágenes, sonidos, etc.) o mediante cualquier otro medio técnico de tratamiento, sea este electrónico o no.

4. Definiciones

Los términos en mayúscula utilizados en este SOP se definen en la Ley Estatutaria 1581 de 2012, salvo que se encuentren definidos de manera diferente en la Sección 4 del presente SOP. En caso de contradicción entre las definiciones contenidas en este SOP y aquellas de la Ley Estatutaria 1581, se aplicarán las contenidas en este SOP.

Datos Personales: Es toda la información que se vincule a una persona o grupo de personas naturales. Es indistinto si la persona a quien se refiere la información puede ser identificada en base a tal información o si es necesario utilizar otra información adicional para poder identificar a la persona. La información adicional puede ser tanto información pública como información contenida en otras bases de datos utilizadas por la Compañía y/o sus proveedores como, por ejemplo, códigos que identifican a pacientes, el 5-2-1, la posición de una persona en una empresa u organización, información periodística, etc.

Datos Sensibles: Son aquellos Datos Personales que afectan la intimidad del Titular o cuyo uso indebido pueda dar lugar a discriminación. En particular, se consideran Datos Sensibles aquellos referidos a la salud, vida sexual, datos biométricos, origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición.

ePA: Es el análisis electrónico de privacidad que se realiza en conjunto entre uno o más asociados y un profesional del departamento de Data Privacy en el cual se analizan las actividades de tratamiento, los potenciales riesgos que presentan las mismas y se establecen

medidas para mitigar los mismos. Existen ePAs globales, regionales y locales y pueden referirse a actividades puntuales o a categorías de actividades. En determinadas situaciones, un ePA global puede a su vez complementarse con preguntas y lineamientos contenidos en herramientas específicas para gestionar determinados procesos como ser POPSys o One Registry.

5. Área que asume la función de protección de datos personales

En cumplimiento de las disposiciones del artículo 23 del Decreto 1.377 de 2013, se deja constancia de que el área responsable por la protección de Datos Personales dentro de la Compañía es el departamento de Data Privacy, el cual contará para la consecución de tales funciones con el soporte y apoyo del resto del departamento Legal.

Todos los asociados de la Compañía que Traten Datos Personales deberán seguir en sus actividades de Tratamiento los lineamientos de la Política Global de Privacidad de Novartis, este SOP y, para las cuestiones no previstas en los mismos, las indicaciones que brinde Data Privacy.

6. Recolección y Tratamiento de Datos Personales

El Tratamiento de los Datos Personales sólo puede efectuarse cuando la Ley No. 1581 de 2012 u otras disposiciones legales lo autoricen o el Titular de los Datos consienta expresamente en ello. En consecuencia, salvo excepciones debidamente aprobadas por el departamento de privacidad, los asociados deberán contar con el consentimiento expreso de cada uno de los titulares de los datos previo a la recolección y/o uso de sus datos personales.

a. Consentimiento

En caso de que el Tratamiento de los Datos Personales se funde en el consentimiento del Titular de los Datos, se deberá respetar lo siguiente:

i. Se deberá solicitar el consentimiento de cada uno de los Titulares de los Datos utilizando el último modelo aprobado para el Titular de Datos de que se trate o, en su defecto, un modelo autorizado por escrito (en papel, por email o a través de la herramienta de ePA) por el profesional de Data Privacy con responsabilidad sobre Colombia o quien temporalmente lo reemplace.

ii. En todos los casos en que se Traten datos sensibles, será necesario contar con el consentimiento previo y expreso del Titular de los Datos.

iii. Dado que la información de salud, fotografías, grabaciones, testimonios y/o videos de pacientes o participantes en estudios clínicos son datos sensibles, siempre será necesario el consentimiento previo del Titular de los Datos.

iv. En todos los casos en que la recopilación de los datos personales se funde en el consentimiento, será responsabilidad del asociado que los recopile obtener tal consentimiento, conservarlo en un lugar seguro (siguiendo los lineamientos de ISRM) y ponerlo a disposición del departamento de Data Privacy y de cualquier otra área o colaborador que necesite utilizar esos datos personales.

v. En aquellos casos en que un asociado requiera utilizar datos personales recopilados por otro asociado, deberá asegurarse de que el consentimiento oportunamente

brindado por el Titular de los datos personales autoriza el Tratamiento para el propósito que se pretenda. En caso de duda, se deberá consultar con el departamento de Data Privacy.

b. Tratamiento en base a otra justificación legal

En todos los casos en que el Tratamiento de los Datos Personales no se base en el consentimiento del Titular de los Datos Personales, se deberá consultar previamente con el departamento de Data Privacy y obtener su conformidad.

c. ePA

Previo a cualquier actividad que implique recopilación, uso y/o cualquier otro Tratamiento de Datos Personales se deberá consultar con el ePA Activation Team a través de go/ePA. No podrá darse inicio a la actividad sin contar previamente con (a) una confirmación del ePA Activation Team de que ya existe un ePA aprobado para esa actividad; o (b) la confirmación de la herramienta de ePA de que el ePA específico para esa actividad ha sido aprobado.

7. Pedidos de los Titulares de los Datos Personales

En caso de que los Titulares de los Datos Personales soliciten ejercer los derechos que les reconoce la legislación, se seguirá el siguiente procedimiento:

a. Medios para ejercer los derechos

En todos los casos en que se solicite el consentimiento de un Titular para el Tratamiento de sus Datos Personales, se le indicará que puede ejercer sus derechos escribiendo un email a la dirección: privacidad.datos@novartis.com

Sin perjuicio de lo anterior, se reconoce que los Titulares pueden realizar sus pedidos de cualquier manera en que lo consideren conveniente. Por lo tanto, es responsabilidad de cada asociado identificar aquellas situaciones en que un Titular está solicitando el ejercicio de alguno de sus derechos y dar curso a tal solicitud sin demora, involucrando a Data Privacy en la medida en que sea necesario, según se indica a continuación.

b. Comprobación de identidad

En todos los casos, será necesario comprobar la identidad de quien realiza una solicitud de ejercicio de derechos a fin de confirmar que el pedido es realizado por el Titular de los Datos Personales a los que se refiere el pedido.

La identidad deberá comprobarse, en la medida de lo posible, contrastando información provista por el Titular con la información que sobre el mismo tenga la Compañía y/o solicitando al Titular que brinde alguno(s) datos que la Compañía ya tenga en su poder y que sólo el Titular debería conocer y/o solicitando al Titular que realice su pedido a través de la plataforma o aplicación en la que originalmente haya insertado sus datos.

En caso de que ello no fuera posible, se podrá solicitar una copia del documento nacional de identificación o pasaporte del Titular, la cual deberá utilizarse únicamente con propósitos de verificar la identidad.

En caso de duda sobre la identidad entre el solicitante y el Titular, se deberá consultar con Data Privacy antes de dar curso a la solicitud.

c. Pedidos de actualización, rectificación y/o eliminación

En caso de que un asociado reciba de un Titular un pedido para actualizar, rectificar o eliminar sus Datos Personales, deberá analizar si tal actualización o rectificación impacta a los procesos de la Compañía y/o podría causar perjuicios a derechos o intereses de terceros y/o existe una obligación legal de conservar los datos.

En caso de que no cause impacto a la Compañía ni a los derechos de terceros, ni exista obligación legal de conservar los datos, deberá procederse a la actualización, rectificación o eliminación solicitada y comunicarlo al Titular de los Datos Personales, de igual manera el asociado responsable deberá poner tal circunstancia en conocimiento de Data Privacy enviando un mail a: privacidad.datos@novartis.com

En caso de que la actualización o rectificación cause o pudiera causar impacto a las operaciones de la Compañía y/o a los derechos o intereses de terceros, y/o si existiera una obligación legal de conservar los datos, deberá indicar en el registro que se solicita para actualizar o rectificar que el mismo se encuentra en revisión y contactar sin demora a Data Privacy a fin de evaluar en conjunto el rumbo a seguir respecto del pedido. Adicionalmente, si existe una obligación legal de conservar la información, el asociado deberá involucrar al departamento de Legales y a cualquier otra área involucrada con tal obligación.

d. Pedidos de acceso

En caso de que un asociado reciba de un Titular un pedido de acceso a sus Datos Personales, deberá reunir toda la información que se refiera a o se relacione con el Titular y comunicarse con Data Privacy a fin de trabajar en conjunto con dicha área en la respuesta a la solicitud.

e. Plazos

Teniendo en cuenta que la legislación otorga un plazo de diez (10) días hábiles, prorrogables hasta por cinco (5) días adicionales sólo en situaciones excepcionales, se deberá dar pronta respuesta a las solicitudes de los Titulares. En caso de que un asociado considere que no será posible dar respuesta al Titular dentro del plazo de diez (10) días original, deberá comunicarse con Data Privacy sin demora a fin de elaborar en conjunto con dicha área la comunicación relativa a la extensión del plazo.

8. Registración de Bases de Datos

La legislación prevé que las bases de datos deben ser registradas ante la Superintendencia de Industria y Comercio. Es responsabilidad de cada asociado que cree una base de datos informarlo a Legales y Data Privacy dentro de los quince (15) días siguientes a la creación con fin de que puedan proceder a dar cumplimiento a las formalidades del registro.

Adicionalmente, los asociados que sean responsables de una base de datos ya registrada deberán brindar información sobre la misma que les soliciten Legales y/o Data Privacy, así como brindar proactivamente a tales departamentos información sobre cambios en la base de datos (por ejemplo, nuevos usos a brindar a los datos, cambio de ubicación física o tecnología utilizadas para la administración de la base, etc.) así como informar un reemplazante en caso de cambio de posición. En caso de finalización del empleo de un asociado responsable de una base de datos, la designación del reemplazante es responsabilidad del manager.

9. Modelos

Salvo que tengan una autorización expresa de Data Privacy para utilizar una versión diferente, los siguientes modelos de documentos deberán ser utilizados por los asociados en las diferentes actividades de recolección de datos personales que realicen, según corresponda:

Anexo I: Cláusulas de Protección de Datos para contratos de prestación de servicios;

Anexo II: Política de Privacidad para Sitios Web y Aplicaciones;

Anexo III: Consentimiento Informado para HCPs;

Anexo IV: Diapositiva para Presentaciones cuando un evento no requiere un Pre-registro;

Anexo V: Consentimiento Informado PSP.

Los modelos indicados precedentemente podrán ser modificados durante el período de validez del presente SOP por lo cual los asociados deberán descargar el modelo más reciente del SharePoint correspondiente.

10. Confidencialidad de la Política y este SOP

Debido a que la Política Global de Privacidad de Novartis y este SOP contienen información sobre el funcionamiento interno de la Compañía que no resulta necesario ni conveniente compartir con terceros ajenos a la misma, la Compañía ha tomado la decisión de aprovechar la posibilidad que le brinda el artículo 14 del Decreto 1377 de 2013 y publicar solamente un Aviso de Privacidad en su página corporativa.

Tanto la Política Global de Privacidad de Novartis como este SOP y demás documentación interna complementaria se deberán poner a disposición de las autoridades en caso de que resulte necesario, procurando preservar su confidencialidad.

11. Preguntas e Interpretación

Las dudas que se tengan sobre la interpretación de las políticas o del procedimiento deberán ser dirigidas al Data Privacy Officer local.

12. Fecha de Entrada en Vigencia de la Presente Política y Período de Vigencia de la Base de Datos

Este SOP ha sido diseñado y aprobado de acuerdo con lo establecido por la legislación de la República de Colombia y podrá ser modificada o ajustada cuando las circunstancias legales o fácticas así lo requieran.

La presente versión entrará en vigencia el día 1 de mayo de 2022.

Cualquier cambio sustancial en los procedimientos acá descriptos será comunicado oportunamente y de manera eficiente, antes de su implementación.

13. Manejo de Excepciones, Desvíos y Régimen de Consecuencias

Por definición las políticas son obligatorias y la imposibilidad o incapacidad para cumplirlas exige una aprobación previa de la excepción por parte de Data Privacy y ERC.

Tanto para solicitar excepciones como en caso de que se identifique con posterioridad que ha existido una desviación del procedimiento, deberán seguirse los lineamientos establecidos en el Procedimiento Operativo Estandarizado Administración Incumplimientos y Régimen Consecuencias.

Adicionalmente, si dicha desviación genera una sospecha de vulneración a la privacidad de los datos y/o a la legislación aplicable, deberá generarse el reporte correspondiente a través de go/securityincident.

14. Control de Cambios

El presente SOP reemplaza en su totalidad al vigente hasta el día 30 de abril de 2022, estableciendo la aplicación directa de la Política Global de Privacidad de Novartis e incluyendo únicamente aquellas cuestiones que es necesario establecer a fin de dar cumplimiento a requerimientos específicos de la legislación colombiana.