Política y Procedimiento Administrativo Cluster Andino

Manejo y Protección de Información Personal

Realizado por:

Jaramillo Varon Juan Sebastian
Digitally signed by Jaramillo Varon Juan Sebastian
DN: SERIALNUMBER=1750542 + CN=Jaramillo Varon Juan Sebastian, OU=PH, OU=people, DC=novartis, DC=com
Reason: I am the author of this document.
Date: 2016.12.07 15:56:52 -5:00

Juan Sebastián Jaramillo
Abogado

Aprobado por:

Forero Velasquez Ximena Margarita
Digitally signed by Forero Velasquez Ximena Margarita
DN: SERIALNUMBER=634601 + CN=Forero Velasquez Ximena Margarita, OU=PH, OU=people, DC=novartis, DC=com
Reason: I am approving this document.
Date: 2016.12.07 15:16:02 -5:00

Ximena Forero
Legal Head/DPO Andean Cluster

Barragan Sanabria Edgar
Digitally signed by Barragan Sanabria Edgar
DN: dc=com, dc=novartis, ou=people, ou=NB, serialNumber=841904, cn=Barragan Sanabria Edgar
Reason: I am approving this document
Date: 2016.12.07 13:35:26 -05'00'

Edgar Barragan
IGM Colombia/Venezuela

TROYA FLORES CRISTIAN
Digitally signed by TROYA FLORES CRISTIAN
DN: SERIALNUMBER=869277 + CN=TROYA FLORES CRISTIAN, OU=PH, OU=people, DC=novartis, DC=com
Reason: I am approving this document.
Date: 2016.12.07 10:58:09 -5:00

Cristian Troya
DPO PEEC

Miranda Norma
Digitally signed by Miranda Norma
DN: SERIALNUMBER=1638048 + CN=Miranda Norma, OU=PH, OU=people, DC=novartis, DC=com
Reason: I am approving this document.
Date: 2016.12.07 11:47:24 -5:00

Hurami Miranda
IGM PEEC

Madrigal Tavera Dumar Daniel
Digitally signed by Madrigal Tavera Dumar Daniel
DN: SERIALNUMBER=779679 + CN=Madrigal Tavera Dumar Daniel, OU=NB, OU=people, DC=novartis, DC=com
Reason: I am approving this document.
Date: 2016.12.07 17:13:52 -5:00

Dumar Madrigal
BPC Coordinator

Table of Contents

1. PROPÓSITO

Esta política establece una norma común sobre la apropiada protección de la información personal, asimismo, proporciona los principios generales respecto a los derechos de privacidad de los individuos y a las razonables salvaguardas de su información personal. Como empresa dedicada al cuidado de la salud, Novartis trata con cuidado especial la información médica personal y otro tipo de información sensible.

2. ALCANCE

Esta política aplica en Novartis

Colombia:

1. Pharma

1.2 Oncología

2. Sandoz

3. Alcon

Perú y Ecuador:

1. Pharma

1.2 Oncología

2. Sandoz

3. REFERENCIAS

Novartis De Colombia S.A.:

- Constitución Política de Colombia, artículo 151, 202
- Ley 1266 de 20083
- Ley 1273 de 20094
- Ley 1581 del 17 de Octubre del 2012
- Decreto 1377 del 2013

Novartis Biosciences Perú S.A.:

- Ley No 29733 de protección de Datos Personales (promulgada el 03 de Julio de 2011).

- Reglamento DS 003-2013 JUS de la ley de Protección de Datos Personales

Novartis Ecuador S.A:

- Constitución de la Republica de Ecuador.

- Ley de Comercio Electrónico, Firmas y mensajes de datos

- Ley de Sistema Nacional De Registro de Datos Públicos

Políticas y Procedimientos Corporativos

- Código de Conducta

- Politica de BPO

- Novartis Policy on the Protection of Personal Information.

- Manual to the Novartis Policy on the Protection of Personal Information regarding cross-border data flows.

- Novartis Biding Corporate Rules (BCR/ Normas Corporativas Vinculantes)

- Company Level Controls (CLC)

- IGM Policy Framework

4. DEFINICIONES, GLOSARIO Y ABREVIATURAS

- **Binding Corporate Rules / Normas Corporativas Vinculantes (BCR):** Son los principios que regulan la transferencia de datos personales entre entidades del Grupo Novartis que aplican cuando los datos se tratan en el European Economic Area (EEA).

- **Base de Datos:** Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico y otros que se creen, cualquiera fuera la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.

- **Habeas Data:** Es el derecho que tienen todas las personas de conocer, actualizar y rectificar, así como de oponerse al procesamiento de sus datos, cancelarlos o revocar su autorización, anular, en caso corresponda, los datos personales que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

- **Flujo Transfronterizo de datos personales.** Transferencia internacional de datos personales a un destinatario situado en un pais distinto al pais de origen de los datos personales, sin importar el soporte en que éstos se encuentren, los medios por los cuales se efectuó la transfrencia ni el tratamiento que reciban.

- **Encargado/Receptor del Tratamiento: Persona** natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- **Responsable del Tratamiento**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y /o el Tratamiento de los datos.

- **Titular de los datos personales:** Persona natural cuyos datos personales sean objeto de Tratamiento.

- **Tratamiento o Procesamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión o cualquier operación o conjunto de operaciones que se lleve a cabo a partir de información personal, sea o no por medios automáticos tales como recopilación, registro, organización, almacenaje, adaptación o alteración, recuperación, consulta, uso, divulgación por transmisión, difusión o que de alguna otra forma permita la alineación o combinación, bloqueo, borrado o destrucción.

- **BPO:** Business Practices Officer – Oficina de Prácticas de Negocio.

- **Data Privacy Officer:** Coordinar que las actividades de la organización cumplan con la política y las normas locales vigentes en materia de manejo de información personal.

- **Responsable de base de datos en Novartis (database owner):** Es la persona responsable, internamente dentro de la compañía, de una base de datos y de asegurar que su manejo se realiza en cumplimiento de las políticas y normas que le sean aplicables de acuerdo a la legislación local.

- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables.

- **Datos personales sensibles:** Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, ingresos económicos, opiniones políticas, preferencia sexual.

- **Consentimiento:** Manifestación de la voluntad del titular de los datos personales mediante el cual autoriza la recolección, procesamiento, uso, disposición, y la transferencia de su información personal con un fin específico de acuerdo a legitimación jurídica de cada País del Cluster Andino. En caso de recopilar datos personales sensibles, las Autorizaciones/Consentimientos deberán ser otorgadas de acuerdo a cada legislación local.

-Incidente de Seguridad de datos significativo:

- La pérdida o mal uso de información personal y sensible.
- Acceso o manipulación de información personal y sensible, fuera de ley, accidental o no autorizado.
- Cualquier acto u omisión que compromete la seguridad, confidencialidad, disponibilidad y/o integridad de la información personal.

- **Procedimiento de anonimización:** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

-**Procedimiento de disociación.** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.

-**Receptor e importador de datos personales.** Es toda persona natural o jurídica de derecho privado, incluyendo las sucursales, filiales, vinculadas o similares; o entidades públicas, que recibe datos personales en caso de transferencia internacional, ya sea como titular o encargado del banco de datos personales, o como tercero.

-**Rectificación.** Es aquella acción genérica destinada a afectar o modificar un banco de datos personales ya sea para actualizarlo incluir información en el o específicamente rectificar su contenido con datos exactos.

- **Base de datos de bases de datos**. Es una plataforma creada para el registro y control de las bases de datos de la compañía, donde se inscribirán cada una de las bases de datos del database owner (*aplica solo para Colombia)

5. RESPONSABILIDADES

5.1. ASOCIADOS

Conocer los principios generales de privacidad, las políticas y procedimientos de Novartis.

Proteger los datos personales de clientes, pacientes, asociados, socios, comerciales y terceros en general.

Consultar al Data Privacy Officer para dudas de Protección y Privacidad de Datos Personales.

Reportar incidentes de privacidad de datos al BPO y Data Privacy Officer oportunamente.

Reportar la creación o modificación (incluyendo circunstancias tales como tipo de información recabada, compartición, custodia, utilización, etc.,) de cualquier Base de Datos al Data Privacy Officer, de acuerdo con el requerimiento de cada País.

Para el caso de los Asociados en Colombia, tendrán la obligación de registrar en la "Base de Datos de Bases de Datos" todas las bases que tengan bajo su responsabilidad.

5.2. TITULARES DE LAS BASES DE DATOS, RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO/PROCESAMIENTO DE INFORMACIÓN PERSONAL

Deberán cumplir con los siguientes deberes:

- Garantizar a los Titulares de datos personales, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

- Implementar los mecanismos para solicitar, recopilar y conservar, en las condiciones previstas en cada legislación local, las Autorizaciones/Consentimientos otorgados por los Titulares de datos personales. En caso de recopilar datos personales sensibles, las Autorizaciones/Consentimientos deberán ser otorgadas por escrito y por cualquier método legal de cada País.

- Informar debidamente al Titular de datos personales sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

- Conservar la información personal bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, mediante medidas físicas, técnicas, organizativas y legales adecuadas.

- Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.

- Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de las políticas de la compañía y de las normas locales.

- Rectificar la información cuando sea incorrecta.

- Informar al Data Privacy Officer cuando determinada información se encuentre en discusión por parte del Titular de datos personales, o se presente cualquier reclamación por parte de terceros.

- Informar a solicitud del Titular de datos personales sobre el uso dado a sus datos.

- Informar al Data Privacy Officer cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

5.3. COUNTRY DATA PRIVACY OFFICER

- Contacto principal para dudas de privacidad de datos en el país.

- Coordinar y apoyar una organización de privacidad a nivel país.

- Dar apoyo al negocio para cumplir con políticas de Novartis y leyes de privacidad.

- Dar apoyo al negocio para implementar procesos de privacidad de acuerdo con leyes locales y necesidades del negocio.

- Dirigir y coordinar el desarrollo de políticas, procedimientos y entrenamientos de privacidad.

- Entrenar a la organización local.

- Atender temas del día a día de privacidad de datos.

- Interactuar con autoridades de protección de datos locales, asegurar que se envían las notificaciones correspondientes.

- Mantenerse actualizado en la regulación de privacidad, interpretación local, desarrollo y tendencias en cada País del Cluster Andino.

- Elaborar e implementar el Sistema para administrar riesgos del tratamiento de información personal.

- Impulsar una cultura de protección de datos dentro de la organización, siendo el enlace y coordinador de la implementación del Programa.

- Registrar las base de datos ante la Entidad Pública, cuando cada legislación local lo requiera.

- Velar por la implementación de planes de auditoria interna para verificar el cumplimiento de las políticas de privacidad de datos.

6. POLÍTICAS

6.1 PRINCIPIOS ORIENTADORES

El manejo de datos personales se regirá al menos por los siguientes principios, sin perjuicio de la existencia de otros:

a) **Principio de Legalidad:** Cumplir con todos los requerimientos legales locales e internacionales respecto a la recolección, procesamiento y disposición final de la información personal, así como las políticas internas de la compañía.

b) **Principio de Finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser consentida explícitamente por el Titular de datos personales en su Autorización. Se entenderá que la finalidad del tratamiento es determinada cuando sin lugar a confusión se especifique en qué consiste el tratamiento.

Recolectar información personal sólo por medios legales y justos, y procesar la información personal de manera compatible con el propósito para el cual fue recopilada. Se deberá señalar en el aviso de privacidad de forma clara y concreta la finalidad o finalidades del tratamiento de información personal.

c) **Principio de Consentimiento:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso, informado e inequívoco del Titular de datos personales. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. Los casos en los que el Tratamiento esté exento de Autorización previa serán los previstos en cada legislación pertinente local.

d) **Principio de veracidad o calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, según se requiera para el cumplimiento de la finalidad para la cual es tratada. Se prohíbe el Tratamiento de datos parciales,

incompletos, fraccionados o que induzca a error.
Sólo la información personal que es relevante para las finalidades autorizadas (ninguna más), será recolectada y procesada. Se debe proporcionar a los individuos la oportunidad de acceder a la información personal relativa a ellos y, en la medida que sea aplicable, satisfacer las solicitudes para corregir, modificar o rectificar la información personal, cuando ésta sea incompleta, inexacta o que no cumpla con los procedimientos estándar de operación. Se pueden aplicar restricciones por razones reglamentarias o legales.

e) **Principio de transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia y características principales del Tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad.

f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de leyes y Constituciones locales. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en las s Leyes pertinentes.

Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares de datos personales o terceros autorizados conforme a las leyes locales.

g) **Principio de seguridad: La** información sujeta a Tratamiento por el Responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Se podrá compartir información personal, tal como permitir el acceso, transmisión o publicación a terceras personas (tanto dentro como fuera de Novartis) solamente con la garantía razonable de que el receptor aplicará medidas de protección de privacidad y seguridad a la información personal. Esto puede incluir protecciones y controles contractuales.

h) Principio de confidencialidad: Novartis tiene la obligación de garantizar la reserva de la información, inclusive después de finalizadas las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

I) Principio de Lealtad: Establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. Por ningún motivo se podrán utilizar medios engañosos o fraudulentos para conseguir y tratar datos personales. Se considerará que se actúa de manera fraudulenta o engañosa cuando:

- Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento de los datos personales.
- Se vulnere la expectativa razonable de privacidad o las finalidades no fueron las

establecidas en el aviso de privacidad.

j) Compartición de Información Personal y Transferencia de información: la transmisión o publicación a terceras personas (tanto dentro como fuera de Novartis) solamente podrá realizarse con la garantía razonable de que el receptor aplicará una protección de privacidad y seguridad a la información personal. Esto puede incluir protecciones y controles contractuales. Así mismo se deberán cumplir con todas las restricciones y requerimientos que se apliquen a la transferencia nacional e internacional de información personal y en estricta concordancia con cada regulación local.

6.2 CONSENTIMIENTO

Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, el cual debe ser previo e informado, salvo las excepciones establecidas en la legislación local de protección de datos personales.

Al momento de obtener el consentimiento del Titular de la Información, se le deberá informar de manera clara y expresa lo siguiente:

- El tratamiento al cual serán sometidos sus datos personales y la finalidad o finalidades autorizadas;
- Si se requiere compartir o transferir la información con otros destinatarios, la Autorización deberá prever dicha circunstancia, así como se deberá asegurar que dichos destinatarios cumplan con las normas de protección de datos personales. En caso los destinatarios estén ubicados en un país distinto al del lugar donde se recopila la Autorización, deberá informarse de dicha situación al Titular de datos personales.
- En caso se recaben datos sensibles, la Autorización correspondiente deberá constar por escrito.
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando éstas versen sobre datos sensibles o sobre los datos de menores de edad.
- Las derivaciones de no otorgar la Autorización para el tratamiento de datos personales,
- La identificación, dirección física o electrónica y teléfono del Titular de la base de datos y del Responsable de su Tratamiento.
- Se deberá informar igualmente los derechos que tiene como Titular de datos personales, entre ellos, el derecho de corrección, modificación, actualización, acceso a su información y revocatoria del consentimiento así como el retiro de la información brindada. (Salvo las excepciones contempladas en la ley).

6.3 TRATAMIENTO DE DATOS PERSONALES

El Tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades

previstas en la Autorización. Si es necesario tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

El Tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

El Responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al Titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

6.4 TRATAMIENTO DE DATOS SENSIBLES

Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

a) El Titular haya dado su autorización explícita a dicho Tratamiento por escrito, salvo en los casos que por ley local no sea requerido el otorgamiento de dicha Autorización.
b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su Autorización.
c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.
d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.
Todo el tratamiento de datos sensibles, deben ajustarse estrictamente con cada legislación local.

6.5 DERECHOS DE LOS TITULARES DE INFORMACIÓN PERSONAL

El Titular de los datos personales tendrá los siguientes derechos:
a) Conocer, acceder, actualizar y rectificar sus datos personales frente a los Titulares de los bancos de datos,

Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros casos, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la Autorización otorgada al Titular del banco de datos, Responsable del Tratamiento salvo cuando expresamente se exceptúe por disposiciones legales o por decisión de autoridad competente.

c) Ser informado por el Titular del banco de datos, Responsable del Tratamiento y/o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

d) Revocar parcial o totalmente la Autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

e) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

6.6 PROCEDIMIENTO PARA EL EJERCICIO DE SUS DERECHOS COMO TITULAR DE DATOS

Los derechos de los Titulares establecidos en cada Ley local, podrán ser ejercidos ante NOVARTIS únicamente mediante los Canales Habilitados definidos, de acuerdo con las siguientes previsiones:

El Titular de los datos deberá acreditar ante NOVARTIS su identidad o, en su defecto, su representante y/o apoderado deberá acreditar ante NOVARTIS el otorgamiento de facultades suficientes.

Consultas:

- Los Titulares o Representantes podrán consultar la información personal del Titular que se encuentre en nuestras bases de datos.
- La consulta se realizará a través de los medios que se han dispuesto por parte de Novartis y que se describen en Canales Habilitados y autorizados.

- La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Los cuales podrán ser prorrogables en un término máximo de cinco (5) días siguientes al vencimiento del primer término, luego de informar previamente al interesado, expresando los motivos de la demora.

Reclamos o Modificaciones:

Los Titulares de la información que consideren que la información que se encuentra contenida en las bases de datos de Novartis Colombia y Perú debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la legislación vigente, podrán presentar una solicitud, la cual surtirá las siguientes reglas:

- Al reclamo deberá adjuntarse fotocopia del documento de identificación del Titular de los datos

- El reclamo se formulará mediante solicitud escrita dirigida a Novartis con la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañado de los documentos necesarios para soportar la situación.

- El reclamo se formulará a través del canal que para dicho efecto ha sido habilitado, el cual se describe en los "canales habilitados".

- Si el reclamo no cumple con los requisitos descritos, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo, para que realice las modificaciones pertinentes.

- El término máximo para atender el reclamo por parte de Novartis Colombia y Perú será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Los cuales podrán ser prorrogables en un término máximo de cinco (5) días siguientes al vencimiento del primer término, luego de informar previamente al interesado, expresando los motivos de la demora.

Para Novartis Biosciences Perú:

Adicionalmente existen plazos máximos de reclamos o modificaciones:

a. Derecho de información: ocho (08) días hábiles.
b. Derecho de acceso: veinte (20) días hábiles.
c. Derecho de oposición: diez (10) días hábiles.
d. Derecho de rectificación: diez (10) días hábiles
e. Derecho de cancelación: diez (10) días hábiles.
f. Revocación de la totalidad del tratamiento: diez (10) días hábiles.
g. Revocación parcial del tratamiento: cinco (5) días hábiles.

Canales Habilitados:

Los derechos de los Titulares podrán ser ejercidos por las personas antes señaladas a través de los canales que han sido habilitados por Novartis para dicho efecto, el cual se encuentran a su disposición de forma gratuita.

COLOMBIA: A través de la dirección de correo electrónico: privacidad.datos@novartis.com

ECUADOR: A través de la dirección de correo electrónico: datospersonales.ecuador@novartis.com

PERÚ: A través de la dirección de correo electrónico: datospersonales.peru@novartis.com

6.7 BASES DE DATOS

6.7.1 Responsable de la base de datos en Novartis (database owner)

- Cada base de datos deberá tener asignado en todo momento a un Database Owner y deberá ser notificada y registrada frente al Data Privacy Officer, además de notificar en caso de cambios de owner.

- Asegurarse que la base de datos se crea y administra de acuerdo a la política de protección de datos personales.

- Realizar una evaluación de riesgo utilizando el "High Level Classification & Consultation Document" (HLCCD), en el caso que la evaluación determine que la base de datos es relevante para datos personales, deberá completar el "Privacy Impact Assessement" antes de crear una base de datos.

- Es obligatorio que exista un reporte de la base de datos al Data Privacy Officer para que la base de incluya en el inventario de bases de datos personales.

- Notificar al Data Privacy Officer / Coordinator de los cambios de responsable de la base de datos (Database Owner).

- Informar al Data Privacy Officer / Coordinator de cualquier cambio en la base de datos, tales como: inclusión de información, decisión de transferir el tratamiento de datos personales a un tercero, cambio de servidor, acceso a terceros de la información, cambio en el tratamiento de los datos personales.

- Eliminar la base de datos o datos personales cuando: la finalidad de tratamiento haya terminado, a petición de Data Privacy Officer, se cumpla el término señalado en esta Política para las bases de datos, luego de considerar que no se va a renovar o por el ejercicio de los derechos del titular. Mantener las medidas de seguridad en la base de datos de acuerdo a la Política de Seguridad de la Información.

- Asegurar que solo tengan acceso a la base de datos aquellas personas que hayan sido definidas con la "necesidad de saber", comunicarles el aviso de privacidad aplicable a la base de datos y solicitar la firma de la carta de confidencialidad de la base de datos.

6.7.2 Creación base de datos

Antes de crear una base de datos, el Database Owner deberá: (Guideline regarding the set-up and management of databases containing Personal Information).

- Realizar una evaluación de riesgo utilizando el "High Level Classification & Consultation Document" (HLCCD).

- Contactar al Data Privacy Officer/Coordinator El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recaudados.

- Contar con los respectivos consentimientos específicos de los Titulares de la información, de acuerdo a la pertinencia de cada legislación local, de tal forma que cuando sean requeridos estén a

disposición.

6.7.3. Cambios y eliminación de bases de datos

El database owner deberá informar al Data Privacy Officer cualquier cambio en la base de datos, tales como: inclusión de información, decisión de transferir el tratamiento de datos personales a un tercero, cambio de servidor, acceso a terceros, cambio en el tratamiento de los datos personales, incorporación de nueva información personal o información personal sensible.

6.8 PROCESAMIENTO DE DATOS POR PARTE DE TERCEROS

En el evento que la Compañía contrate los servicios de un tercero para que recolecte y administre datos personales a nombre de la compañía, le será aplicable a dicho tercero las normas y principios incluidos en la presente política así como las disposiciones locales vigentes. Estas obligaciones deberán ser incorporadas en el contrato que se suscriba con el tercero.

El contrato que suscriba Novartis como Titular de la base de datos o Responsable de la información con los Encargados para el Tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del Tratamiento, las actividades que el Encargado realizará por cuenta del Responsable para el Tratamiento de los datos personales y las obligaciones del Encargado para con el Titular y el Responsable.

6.9 TRANSFERENCIA DE DATOS A TERCEROS PAISES

Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por cada autoridad local sobre la materia:

1) Que existan normas constitutivas de derechos en cabeza del Titular de datos y obligaciones respecto de quienes hagan tratamiento o ejercen control sobre el mismo y 2) que se cuente con los mecanismos necesarios que garanticen la aplicación de las normas, lo cual implica el establecimiento de un conjunto de sanciones a los infractores y un órgano de control. Esta prohibición no regirá cuando se trate de:
a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca

para la transferencia.

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública.

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable. d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

6.9.1 TRANSFERENCIA DE DATOS ENTRE ENTIDADES DE NOVARTIS

Las transferencias nacionales o internacionales de datos personales entre entidades de Novartis se regirán por las Binding Corporate Rules (Normas Corporativas Vinculantes) de Novartis. Éstas contemplan la obligatoriedad de acuerdos de transferencia específicos, entre aquellas entidades de NOVARTIS que ejecutan la transferencia. Los BCR complementan la Política Global de Protección de Información Personal de Novartis y tienen el objetivo de asegurar un nivel adecuado de protección para el tratamiento de datos personales entre compañías del Grupo Novartis.

6.10 INCIDENTES RELACIONADOS CON EL MANEJO DE INFORMACION PERSONAL

Se consideran como incidentes de seguridad de datos personales:

- La pérdida o uso indebido de datos personales.
- El robo, extravío o copia no autorizada de información personal.
- El acceso, uso o tratamiento no autorizado, ilegal o accidental de datos personales.
- El daño, alteración o modificación no autorizada de los datos.
- Cualquier otro acto u omisión que comprometa la seguridad, integridad o confidencialidad de datos personales.
- La recopilación de información personal sin consentimiento previo cuando este se requiera.

Estos incidentes pueden presentarse respecto a información que se encuentre almacenada en cualquier medio sea electrónico o en papel.

Estos incidentes incluyen tanto la información personal manejada directamente por Novartis como aquella que se recopila o administra por un tercero en virtud de un contrato con la compañía.

Los incidentes de datos personales se deben reportar de acuerdo al procedimiento de BPO y al Data Privacy Officer para que se determinen las medidas que haya a lugar.

6.11 COMITÉ DE RESPUESTA PARA LOS INCIDENTES

El comité estará encargado de las siguientes funciones:

- Revisar e investigar las circunstancias del incidente.
- General las repuestas de los respectivos incidentes.
- Asegurar los sistemas afectados
- Revisar y reportar, de acuerdo con los requerimientos legales, el incidente
- Implementar obligaciones legales aplicables así como las notificaciones requeridas a la autoridad gubernamental y al titular de la información.

El comité estará conformado por:

- Departamento Legal/Data Privacy Office local
- IGM
- Control Interno en los casos que se trate de una mala conducta o fraude.

6.12 PROCEDIMIENTO FRENTE A LOS INCIDENTES RELACIONADOS CON EL MANEJO DE LA INFORMACIÓN.

Una vez se haya generado el reporte, por medio del "Formato de Reporte" Anexo 2 de esta política, el comité designara una persona que haga la investigación correspondiente:

Si existe información personal relacionada con el incidente se debe desarrollar el procedimiento descrito en el Anexo 1 de esta política, en caso de tratarse de un incidente diferente, éste se manejara de acuerdo a los procedimientos generales de IGM.

6.13 ENTRENAMIENTO Y DIFUSIÓN

Todos los asociados deberán realizar un entrenamiento básico de protección de datos personales que incluya los principios básicos, principales requerimientos incluyendo los BCR. Dicho entrenamiento será realizado en la inducción. Además, el grupo de empleados que pertenezca a los cargos críticos definidos por DPO y Compliance Officer podrían recibir un entrenamiento adicional. Finalmente, los asociados que desde Global reciban solicitud de hacer entrenamiento por medio electrónico deberán culminar dicha capacitación en los tiempos definidos por Global.

- Los asociados en funciones específicas incluyendo sin limitar a Legal, Recursos Humanos, IT, Programas de pacientes, Compras, Desarrollo Clínico, Seguridad Corporativa, que tienen acceso regular

y/o tratan datos personales deben recibir entrenamiento específico con las obligaciones que tienen en su área específica incluyendo los BCR.

- Se deberán realizar campañas periódicas sobre temas de protección de datos personales por parte de los Data Privacy Officers, así como mantener las políticas y procedimientos sobre protección de datos disponible en la Intranet para consulta de los asociados.

- Cada vez que exista una actualización de Políticas o legislativa, se comunicará a todos los asociados y se suministrara con más profundidad, capacitación a aquellos que por sus funciones específicas así lo requieran.

6.14 VIGENCIA DEL TRATAMIENTO DE DATOS PERSONALES

Las bases de datos, serán almacenadas por un término que sea razonable y necesario, de acuerdo con las finalidades justificadas en el momento de la recolección de datos, sin embargo cada tres años se hará una revisión de la base de datos, con la finalidad de poder determinar si la finalidad de la base de datos, sigue existiendo. Luego del respectivo procedimiento interno de revisión, se podrá determinar la eliminación de la información. Pudiendo el titular de los datos ejercer sus derechos en cualquier momento.

6.15 SEGURIDAD DE INFORMACIÓN PERSONAL

La información personal debe ser protegida con medidas técnicas adecuadas. Dichas medidas deben ser revisadas periódicamente.

El titular de la base de datos (database owner) deberá asegurar la confidencialidad, disponibilidad e integridad de la información personal así como un nivel de protección adecuada de la misma. Deberá protegerla en particular contra:

- Acceso no autorizado
- Destrucción accidental
- Pérdida de información personal
- Fallas técnicas
- Falsificación, hurto o uso ilegal.
- Alteración, copia, acceso u otro proceso no autorizado sobre dicha información personal.

6.16 MONITOREO DE CUMPLIMIENTO

Para monitorear el cumplimiento de la Política de Protección de Datos Personales se realizarán:

- Evaluación de impacto de Privacidad denominados PIA “Privacy Impact Assessment”,

que se realiza a las diferentes bases de datos que contengan información personal una vez se ha realizado el proceso de evaluación de riesgo de acuerdo con el "High Level Classification & Consultation Document" (HLCCD).

- Evaluación de Cumplimiento de Privacidad (Privacy Compliance Assessment): el Data Privacy Officer podrá realizar en cualquier momento una evaluación de cumplimiento de la política de protección de datos personales. Esta evaluación podrá generar un plan de remediación si hay lugar a ello.
- A criterio del DPO, se podrán realizar revisiones periódicas de las bases de datos, en relación con su vigencia y de igual forma la verificación del almacenamiento de sus respectivos consentimientos previos.

6.17 INCUMPLIMIENTO DE LA POLÍTICA

Dada la importancia de la protección de la información personal y las garantías que Novartis debe suministrar a los titulares de esta, y teniendo en cuenta la obligación que tiene cada uno de los asociados para dar cumplimiento a las políticas de la Compañía, en caso que se presente un incumplimiento a dicha política se aplicará lo establecido en la Política y Procedimiento de Excepciones e incumplimiento y Régimen de Consecuencias.

7. 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.

8. FECHA DE ENTRADA EN VIGENCIA DE LA PRESENTE POLÍTICA Y PERÍODO DE VIGENCIA DE LA BASE DE DATOS

Esta Política de tratamiento fue diseñada y aprobada de acuerdo con lo establecido para cada ley local y podrá ser modificada o ajustada cuando las circunstancias legales o fácticas así lo determinen.

La entrada en vigencia de esta versión, se entenderá a partir del 15 de Enero del 2017, cualquier cambio sustancial en las políticas de tratamiento de la información será comunicada oportunamente y de manera eficiente, antes de implementarse las nuevas políticas.

9. SITUACIONES ESPECIALES

Por definición las políticas son obligatorias y la imposibilidad o incapacidad para cumplir las exige una

aprobación previa de la desviación por parte del DPO y el Compliance Officer o sus delegados. Para que se pueda generar ésta, se debe solicitar por medio del formato de Desviaciones dispuesto por el DPO.

10. MISCELANEA APLICABLE SOLAMENTE PARA LA OPERACION DE NOVARTIS EN COLOMBIA

El Responsable de la base de datos está en la obligación, de mantener actualizado el registro de bases de datos interno. Esto con la intención de poder generar los reportes pertinentes frente a la autoridad que lo pueda llegar a requerir. El registro de bases de datos contendrá por lo menos los siguientes campos:

1. Owner de la base de datos
2. Desde cuando está vigente la base de datos (Primera recolección de datos)
3. Nombre y finalidad de la base de datos.
4. Forma de Tratamiento de la base de datos (manual y/o automatizada).

11. MISCELANEA APLICABLE SOLAMENTE PARA LA OPERACIÓN DE NOVARTIS EN PERU

Transferencia de datos personales

En el caso de transferencias de datos personales dentro de grupos empresariales, sociedades subsidiarias afiliadas o vinculadas bajo el control común del mismo grupo del titular del banco de datos personales responsable del tratamiento, o a aquellas afiliadas o vinculadas a una sociedad matriz o a cualquier sociedad del mismo grupo del titular del banco de datos o responsable del tratamiento, se cumple con garantizar el tratamiento de datos personales, si se cuenta con un código de conducta que establezca las normas intimas de protección de datos personales.

1. En Perú el plazo para la conservación de los datos será de dos (2) años contado desde la finalización del último encargo realizado.

2. Lo mencionado aplica, en to que corresponda, a la subcontratación de la prestación de servicios de tratamiento de datos personales.

3. En Perú, existe el Registro Nacional de Protección de Datos Personales como registro de carácter administrativo a cargo de la Autoridad Nacional de Protección de Datos Personales, con la finalidad de inscribir en forma diferenciada, a nivel nacional, lo siguiente:

i) Los bancos de datos personales de administración pública o privada, así como los datos relativos a estos que sean necesarios para el ejercicio de los derechos que corresponden a los titulares de datos personales.

ii) Las autorizaciones emitidas conforme Ley local.

iii) Las sanciones, medidas cautelares o correctivas impuestas localmente por la Autoridad Nacional de Protección de Datos Personales.

iv) Los códigos de conducta de las entidades representativas de los titulares o encargados de bancos de datos personales de administración privada.

v) Otros actos materia de inscripción conforme al reglamento.

Sanciones administrativas:

De acuerdo a la ley local en caso de incumplimiento o violación a las directivas se aplican las siguientes inultas:

1. Las infracciones leves: desde 0.5UIT hasta 5 UIT.
2. Las infracciones graves: desde 5 UIT hasta 50 UIT.
3. Las infracciones muy graves: desde 50 UIT hasta 100 UIT.

1. Las medidas de seguridad que deben cumplir todo responsable o encargado del tratamiento de datos se encuentran estipuladas en el Capítulo V del Decreto Supremo N° 003-2013-JUS, Reglamento de la Ley de Protección de Datos Personales, y la Directiva de Seguridad publicado por la Dirección General de Protección de Datos.
2. En los casos donde se recopile u ordene el levantamiento de datos personales, el encargado o responsable deberá obtener y dejar constancia del consentimiento de los titulares de datos personales. Los mismos deberán estar a disposición de Novartis para la atención de solicitudes de derechos de ejercicio establecidos en la Ley 29733. Si se recopila el consentimiento a menores de edad, el mismo deberá de ser expreso, escrito y en un mensaje claro dejando constancia de la autorización de los titulares de la patria potestad o tutores.
3. Cuando sea necesario realizar la transferencia de datos personales se deberán tomar las medidas necesarias, entre las que se encuentran cifrado de datos, firmas digitales, información, entre otros, destinados a evitar todo tipo de incidente de seguridad.
4. En todo caso donde se subcontrate a un tercero para realizar el tratamiento de datos personales deberán mediar un contrato o convenio de por medio, por el cual se establezca las finalidades consentidas por el titular y del tratamiento, las medidas de seguridad a las que está sujeto, y la adopción de las conductas necesarias a las políticas de Novartis. En particular, para los casos que aplique, deberán quedar claros los procesos de anonimización o disociación que requiere cierto tipo de información para ser tratado por Novartis, por ejemplo, datos de pacientes o participantes en investigaciones médicas.

12. MISCELANEA APLICABLE SOLAMENTE PARA LA OPERACIÓN DE NOVARTIS EN ECUADOR

Responsabilidad de la información.-

Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de Ia integridad, protección y control de los registros y bases de datos a su cargo.

Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de Ia o el declarante cuando esta o este proveen toda la información.

Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal.

La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución. ("Art. 4 Ley del sistema nacional de registro de datos Públicos.

a) El numeral 11 del Art. 66 de la Constitución Ecuatoriana de Derechos y Justicia, dispone que en ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.

b) Conforme at Art. 92 de la Constitución, establece que toda persona tendrá derecho a conocer datos sobre sí misma, que consten en entidades públicas y privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Para poder difundir la información archivada se requerirá la autorización de su titular o de la ley.

c) El Art. 4 de la Ley del Sistema Nacional De Registro De Datos Públicos, establece que las instituciones del sector público y privado y las personas naturales que administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva del declarante cuando este provee toda la información.

d) El Art. 9 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, establece que el manejo de la recopilación y uso de datos personales deberá ser tratado de conformidad con los derechos de privacidad, intimidad y confidencialidad garantizadas por la Constitución, los cuales podrán ser utilizadas o transferidas únicamente con autorización del titular u orden de autoridad competente.

e) Y el numeral cuarto del Art. 30 de la Ley Orgánica de Comunicación, considera información restringida, a aquella información acerca de los niños y adolescentes que viole sus derechos según lo establecido en el Código de la Niñez y Adolescencia.

Sanciones.-

La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley. ("Ref Art. 178 COIP. Delitos contra el derecho a la intimidad personal y familiar").

13. MANEJO DE EXCEPCIONES Y RÉGIMEN DE CONSECUENCIAS

En caso que el DPO y el compliance Officer o sus delegados considere que existe una desviación del procedimiento, deberá documentarse de acuerdo con los lineamientos establecidos en el Procedimiento de Administración de excepciones y régimen de consecuencias. Sin embargo si dicha desviación genera una sospecha de violación a las políticas de privacidad de datos, el caso debe ser reportado al sistema de reporte BPO.

14. CONTROL DE CAMBIOS

VERSIÓN No.	CAMBIO			AUTORIZACION CAMBIO			
	ITEM	PAGINA	CONCEPTO	FECHA	CARGO	NOMBRE	FIRMA (o indicar medio de