HEALTH & SAFETY IPS

Manual: Manual de politicas web y seguridad de procedimientos

HEALTH&SAFETY IPS PROTEGEMOS TU SALUD	**HEALTH & SAFETY IPS** **Proceso**: Direccionamiento estrategico **Manual**: Manual de politicas web y seguridad de procedimientos	**Código** MA-DE-3 **Fecha** 2025-09-18 **Versión** 2

Estratégico	Misional	Apoyo	Mejoramiento continuo

Objetivo
Garantizar la protección de los datos personales de los titulares, cumpliendo con la normativa vigente y asegurando que la información sea manejada de manera ética y transparente.

Alcance
El manual de política y procedimientos Habeas Data de H&S IPS SAS se aplicará a todas las bases de datos, documentos y/o archivos que contengan datos personales.

Responsable
H&S IPS SAS, identificada con NIT. 900821367-5, con sede principal en la ciudad de Bucaramanga, Calle 62#32-08 correo electrónico: gerencia@hysips.com. es la responsable del tratamiento y protección de los datos obtenidos de sus grupos de interés.

Definiciones
Establecidas en el artículo 3 de la LEPD y el capítulo 25 sección 1 artículo 2.2.2.25.1.3 del Decreto 1074 de 2015.

Acceso autorizado: Autorización concedida a un usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

Autenticación: Procedimiento de verificación de la identidad de un usuario.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Contraseña: Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

Control de acceso: Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.

Copia de respaldo: Copia de los datos de una base de datos en un soporte que permita su recuperación.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: Se entiende por datos sensible aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Encargado 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.

Identificación: Proceso de reconocimiento de la identidad de los usuarios.

Incidencia: Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

Perfil de usuario: Grupo de usuarios a los que se da acceso.

Recurso protegido: Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

Responsable de seguridad: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad. • Sistema de información: Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

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.

Soporte: Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.

Usuario: Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Contenido del documento

1. Base legal y ámbito de aplicación

El derecho a la Protección de los Datos tiene como finalidad permitir a todas las personas conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos Personales (LEPD); en el decreto 1074 de 2015, y capítulo 25 sección 3 Articulo 2.2.2.25.3.2. del decreto 1074 de 2015, por el cual se reglamenta parcialmente la 1581 de 2012.

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una base de datos de una institución, pública o privada, jurídica o natural, ésta se hace mediante el responsable del tratamiento de estos datos y adquiere una serie de obligaciones como son: la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Si bien, la responsabilidad del tratamiento de los datos recae en el responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la institución responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la organización y el Manual de Políticas y Procedimientos de Habeas Data; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar con el cumplimiento de sus obligaciones de seguridad, HEALTH AND SAFETY H&S IPS SAS, nombra a cuatro responsables de seguridad encargados de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en el Manual de Políticas y Procedimientos de Habeas Data.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal

externo de HEALTH AND SAFETY H&S IPS SAS.

Todos los usuarios identificados en el presente documento de Seguridad están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

Tipo de Norma	Número y fecha de expedición	Titulo	Expedida por	Aplicación especifica
Ley Estatutaria	1581 de 2012	"Por la cual se dictan disposiciones generales para la protección de datos personales".	Congreso de la Republica.	Por medio de la cual desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.
Ley	1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"	Congreso de la Republica.	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto	1377 de 2013	"Por medio del cual se reglamenta parcialmente la ley 1581 de 2012"	Presidente de la República de Colombia.	Mediante la cual se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	1074 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo."	Presidente de la República de Colombia.	El Ministerio de Comercio, Industria y Turismo tiene como objetivo primordial dentro del marco de su competencia: formular, adoptar, dirigir y coordinar las políticas generales en materia de desarrollo económico y social del país, relacionadas con la competitividad, integración y desarrollo de los sectores productivos de la industria

2. Principios de la protección de datos

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

Principio de legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), el Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la Ley de Protección de Datos (LEPD):

Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

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 de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

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 la Ley de Protección de Datos (LEPD) y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

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. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el Manual de Políticas y Procedimientos de Habeas Data, de obligado cumplimiento para todo usuario y personal de HEALTH AND SAFETY H&S IPS SAS. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

3. Categorías especiales de datos

3.1 Datos sensibles

Los datos sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos. Según el artículo 6 de la Ley Estatuaria de Protección de datos Personales (LEPD), se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- 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.
- 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.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- 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.

3.2 Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1074 de 2015. En todo caso, el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

3.3 Derechos de los Titulares

De acuerdo con el artículo 8 de la LEPD y al capítulo 25 sección 4 del decreto 1074 de 2015, los Titulares de los datos pueden ejercer una serie de derechos en relación con el tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.
- Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

Derecho de acceso o consulta: Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que les han dado a sus datos personales.

Derechos de quejas y reclamos: La Ley distingue cuatro tipos de reclamos:

- Reclamo de corrección: El derecho del Titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Reclamo de supresión: El derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
- Reclamo de revocación: El derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- Reclamo de infracción: El derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento: Salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD.

Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones: El Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

4. Autorización de la política de tratamiento

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de HEALTH AND SAFETY H&S IPS SAS, en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

5. Responsable del tratamiento

El responsable del tratamiento de las bases de datos objeto de esta política es HEALTH AND SAFETY H&S IPS SAS, cuyos datos de contacto son:

Correo electrónico: siau@hysips.com

Teléfono: 6076985827

HEALTH AND SAFETY H&S IPS SAS, en el desarrollo de sus actividades, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información, HEALTH AND SAFETY H&S IPS SAS realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión, entrega de los datos a terceras entidades a título de encargados o de responsables; esto de acuerdo con el acuerdo al que entre las partes se llegue. Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información de HEALTH AND SAFETY H&S IPS SAS, en todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos de control y auditorías internas y externas y evaluaciones que realicen los organismos de control. Así mismo y en ejecución del objeto social de HEALTH AND SAFETY H&S IPS SAS, los datos personales serán tratados de acuerdo con el grupo de interés y en proporción a la finalidad o finalidades que tenga cada tratamiento, como se describe a continuación:

La siguiente tabla presenta las distintas bases de datos y las finalidades asignadas a cada una de ellas.

Bases de datos y finalidades

SOCIOS

Los datos serán utilizados con las siguientes finalidades: Contiene la información de los socios, Validaciones y análisis relacionadas con el Sistema de Administración de Riesgo de Lavado de Activos y en contra de la Financiación del Terrorismo SAGRLAFT, la prevención contra el soborno transnacional y las demás que la normatividad colombiana disponga; en la transmisión de los datos a las entidades que regulan el negocio en temas tributarios y aduaneros; gestionar trámites como solicitudes, quejas y/o reclamos, reportes a centrales de riesgo por incumplimiento de las obligaciones financieras derivadas de la relación comercial, envío de comunicaciones a través de mensajes de texto y correos electrónico; para llevar un historial de consumo, Uso de imágenes fotográficas y videos con fines corporativos, Gestión comercial, Conocer información del comportamiento de los socios, envío de información de los productos, servicios o novedades de la compañía, Conservar registros históricos de la compañía y mantener contacto comercial; Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente. Las anteriores finalidades son enunciativas y no taxativas.

PACIENTES

Los datos serán utilizados con las siguientes finalidades: Los datos de identificación, socio-demográficos, de tipo clínico entre otros, a los que se accede de su parte, y que se generan para poder prestar los servicios de salud o como resultado de la atención recibida, para la prestación de los servicios de salud, incluyendo los servicios de apoyo diagnóstico y terapéutico, en la investigación clínica y epidemiológica, para brindar información sobre las campañas de salud y de mercadeo de nuestra oferta servicios (apertura de nuevos servicios o novedades de los ya existentes, etc.), las imágenes y videos que se utilizaran en el material audiovisual corporativo, información a los medios de comunicación sobre el estado de salud del paciente, en caso de tratarse de una figura pública, para llevar a cabo actividades de educación al paciente y su familia, enviar información a las Entidades Administradoras de Planes de Beneficios (EPS, ARL, Entes Territoriales, etc.), empresas con las cuales se tienen convenios tales como compañías farmacéuticas, centros de fabricación de materiales ortopédicos, bancos de sangre, outsourcing con los cuales existe vinculación, envío de información mediante mensajes de texto y correos electrónicos, para confirmaciones de citas, resultados de apoyo diagnóstico y terapéutico, información sobre los servicios de salud que requiere el paciente (toma de muestras, tratamientos, prescripción de medicamentos de acuerdo con las indicaciones del médico tratante, etc), uso de los datos en las diferentes actividades de auditoria en salud, tanto las auditorías internas como las externas que se realicen, seguimiento de los pacientes al egreso en su fase pos hospitalaria, envío de información a las entidades extranjeras con las cuales se tienen convenios y las cuales se encuentran incluidas en el listado de la Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio, Valoración nutricional y realización del plan de alimentación con las recomendaciones, uso de imágenes fotográficas y videos con fines corporativos, realizar encuestas de satisfacción de los servicios de salud recibidos, agenda miento de citas, gestión de las comunicaciones radicadas por los pacientes (felicitaciones, quejas, peticiones, y sugerencias) y su seguimiento, para la vigilancia epidemiológica, para la atención de la telemedicina y recolección de las autorización para dicho tratamiento, para la prestación de los servicios de salud, incluyendo los servicios de apoyo diagnóstico (p.e. imágenes diagnósticas, laboratorio clínico, etc.) y terapéutico, en la investigación clínica y epidemiológica, para brindar información sobre las campañas de salud y de mercadeo de nuestra oferta servicios (p.e. apertura de nuevos servicios o novedades de los ya existentes, etc.), en las imágenes y videos que se utilizaran en el material audiovisual corporativo, información a los medios de comunicación sobre el estado de salud del paciente, en caso de tratarse de una figura pública, llevar a cabo actividades de educación al paciente y su familia, enviar información a las

Entidades Administradoras de Planes de Beneficios (EPS, ARL, Entes Territoriales, etc.), empresas con las cuales se tienen convenios, acuerdos entre otros, tales como, centros de fabricación de materiales ortopédicos, bancos de sangre, outsourcing con los cuales existe vinculación, envío de información mediante mensajes de texto y correos electrónicos, para confirmaciones de citas, resultados de apoyo diagnóstico (p.e. reportes de laboratorio clínico, etc.), información sobre los servicios de salud que requiere el paciente (p.e. toma de muestras, tratamientos, prescripción de medicamentos de acuerdo con las indicaciones del médico tratante, etc), uso de los datos en las diferentes actividades de auditoria en salud, tanto las auditorías internas como las externas que se realicen, seguimiento de los pacientes al egreso en su fase pos hospitalización domiciliaria , envío de información a las entidades extranjeras con las cuales se tienen convenios y las cuales se encuentran incluidas en el listado de la Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio, valoración nutricional y realización del plan de alimentación con las recomendaciones médicas, realizar encuestas de satisfacción de los servicios de salud recibidos, agendamiento de citas, gestión de las comunicaciones radicadas por los pacientes (felicitaciones, quejas, peticiones, y sugerencias) y su seguimiento, envío de información con motivos promocionales y/o informativos mediante mensajes de texto y correos electrónicos, las anteriores finalidades son enunciativas y no taxativa.

COLABORADORES

Los datos serán utilizados con las siguientes finalidades: Solicitud de datos concernientes a identificación personal, información de contacto, datos de carácter académico, datos del historial laboral, profesional y financiero, desarrollar adecuadamente el proceso de registro y vinculación laboral, implementar acciones de bienestar laboral; difundir ofertas laborales para participar en procesos internos de selección, comunicar información institucional, ejecutar actividades con fines estadísticos, desarrollar adecuadamente el proceso de actualización de los datos, desarrollar los procesos de inscripción en congresos, eventos o seminarios organizados, adelantar la actualización de datos y verificación de identidad de los trabajadores y sus familiares (pareja, padres e hijos), citar a los aspirantes en proceso de selección a las entrevistas programadas, realización de visitas domiciliarias, verificación de referencias laborales, personales, experiencia laboral y trayectoria profesional, suministro de información a las empresas con la cuales se tiene convenio, confección de artículos de dotación, envío de información a través de mensajes de texto y correos electrónicos, entrega y asignación de equipos a los colaboradores, redacción de informes de gestión humana, proceso de afiliación al sistema de seguridad social y cajas de compensación del colaborador y sus beneficiarios, entrega de referencias laborales, Uso de imágenes fotográficas y videos con fines corporativos, Obtención y suministro de datos de los hijos de los colaboradores en el desarrollo de actividades recreativas y de bienestar a través de la Instituciones o entidades aliadas, Evaluaciones de desempeño, Generación de certificaciones laborales, de ascenso, traslado, entrevista de retiro, en procesos de auditoría y control interno y externo, en la entrega de reportes obligatorios institucionales en entrevistas de retiro, Desactivación de sistemas de información, Uso de huellas digitales y demás datos de salud y/o datos sensibles para los fines misionales, las anteriores finalidades son enunciativas y no taxativas.

PROVEEDORES

Los datos serán utilizados con las siguientes finalidades: Solicitud de ofertas y propuestas económicas para la adquisición de productos y servicios; para el análisis y viabilidad de cada producto y/o servicio, envío de comunicaciones a través de mensajes de texto y correos electrónico; presentación de informes pertinentes a los diferentes entes de control; revisión y verificación de referencias comerciales, gestiones pre contractuales y contractuales, suministro de información en procesos de auditoría interna y externa que se realicen al interior de la institución; envío de información de los productos, servicios o novedades de la fundación, rastreo en bases de datos restrictivas tales como (policía, procuraduría, contraloría, SARLAFT – Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo y las demás que la normatividad colombiana disponga) las anteriores finalidades son enunciativas y no taxativas.

VIDEO VIGILANCIA

Los datos serán utilizados con las siguientes finalidades: monitoreo y control para la vigilancia de entrada, salida y tráfico de personas dentro de la compañía, así como para el control de ingreso y salida de vehículos de los parqueaderos, monitoreo de incidentes, medida de disuasión de conductas irregulares de terceros, monitoreo y control de la prestación de los servicios institucionales, Se realizará el envío de la información otorgada y autorizada por el titular las entidades con las cuales se tienen convenios, estas transferencias estarán siempre mediadas por un documento que garantice que el tratamiento que se le dará a sus datos será el mandado por la normatividad vigente.

6. Datos de navegación

El sistema de navegación y el software necesario para el funcionamiento de esta página web recogen algunos datos personales, cuya transmisión se haya implícita en el uso los protocolos de comunicación de Internet.

Por su propia naturaleza, la información recogida podría permitir la identificación de usuarios a través de su asociación con datos de terceros, aunque no se obtenga para ese fin. En esta categoría de datos se encuentran, la dirección IP o el nombre de dominio del equipo utilizado por el usuario para acceder a la página web, la dirección URL, la fecha y hora y otros parámetros relativos al sistema operativo del usuario.

Estos datos de utilizan con la finalidad exclusiva de obtener información estadística anónima sobre el uso de la página web o controlar su correcto funcionamiento técnico, y se cancelan inmediatamente después de ser verificados.

7. Cookies o web bugs

Este sitio web no utiliza cookies o web bugs para recabar datos personales del usuario, sino que su utilización se limita a facilitar al usuario el acceso a la página web. El uso de cookies de sesión, no memorizadas de forma permanente en el equipo del usuario y que desaparecen cuando cierra el navegador, únicamente se limitan a recoger información técnica para identificar la sesión con la finalidad de facilitar el acceso seguro y eficiente de la página web. También se utilizarán para mejorar tus experiencias, entender cómo se usan nuestros Servicios y personalizarlos. Por ejemplo, usamos cookies para proporcionar nuestros Servicios y otros servicios basados en los usos de nuestra página de Internet. También podemos usar las cookies para entender cuáles son los artículos más populares de nuestro Centro de ayuda con el fin de mostrarte el contenido relevante relacionado con nuestros Servicios. Adicionalmente, podemos usar cookies para recordar las opciones que elegiste, como las preferencias de idioma, a fin de proporcionarte una experiencia más segura y, de otro modo, para personalizar nuestros Servicios según tus intereses.

Si no desea permitir el uso de cookies puede rechazarlas o eliminar las ya existentes configurando su navegador, e inhabilitando el código Java Script del navegador en la configuración de seguridad.

8. Atención a los Titulares de datos

Coordinador SIAU, será el encargado de la atención de peticiones, consultas y reclamos ante la cual el titular de los datos puede ejercer sus derechos, en el siguiente Correo electrónico: siau@hysips.com.

9. Procedimientos para ejercer los derechos del Titular

9.1 Derecho de acceso o consulta

De acuerdo con el capítulo 25 sección 4 articulo 2.2.2.25.4.2. 21 del Decreto 1074 de 2015, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

Al menos una vez cada mes calendario.

Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, HEALTH AND SAFETY H&S IPS SAS, solamente podrá cobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a HEALTH AND SAFETY H&S IPS SAS, enviado, mediante correo electrónico a siau@hysips.com, indicando en el asunto “ejercicio del derecho de acceso o consulta, la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento.

Una vez recibida la solicitud, HEALTH AND SAFETY H&S IPS SAS, resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

9.2 Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a HEALTH AND SAFETY H&S IPS SAS, mediante el correo electrónico siau@hysips.com, indicando en el asunto “ejercicio de las quejas y/o reclamos”, la solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

HEALTH AND SAFETY H&S IPS SAS, resolverá la petición de consulta en un plazo máximo de quince

(15) días hábiles contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

10. Medidas de seguridad

HEALTH AND SAFETY H&S IPS SAS, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, HEALTH AND SAFETY H&S IPS SAS, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

11. Vigencia

Las bases de datos responsabilidad de HEALTH AND SAFETY H&S IPS SAS, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. HEALTH AND SAFETY H&S IPS SAS, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, dicha base de datos ha sido creada sin un periodo de vigencia definido.

Documento Relacionados

NO APLICA

Referencias

Ley 1581 de 2012 por la cual se regula la protección de datos personales en Colombia. Define los principios, derechos de los titulares y obligaciones de los responsables y encargados del tratamiento.

1273 de 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”

Decreto 1377 de 2013: por el cual reglamenta la Ley 1581 y establece los requisitos para la inscripción de las bases de datos ante la Superintendencia de Industria y Comercio.