4.20 HIPAA, Health Insurance Portability and Accountability Act.

Introducción. HIPAA es la Ley de Portabilidad y Responsabilidad del Seguro Médico, aplicable en Estados Unidos, su objetivo fundamental es facilitar a las personas mantener un seguro médico, proteger la confidencialidad y seguridad de la información médica, y ayudar a la industria de la salud a controlar los costos administrativos.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
RESPONSABLE						
1	Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.	Art. 6	Art. 9	1. Recomendación General.	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
LICITUD Y LEALTAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
2	Los datos personales deberán recabarse y tratarse de manera lícita, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, sin importar la fuente de la que se obtienen los datos. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.	Art. 7	Art. 7 Art. 10 Art. 44	Paso 1. Alcance y Objetivos.	164.502 Usos y revelaciones de información protegida de salud: Reglas generales.	Disposiciones para usos y revelaciones solamente autorizados con respecto a la información de salud.
CONSENTIMIENTO						
3	El tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley. Los datos financieros o patrimoniales requerirán consentimiento expreso de su titular. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.	Art. 8	Art. 11 Art. 12 Art. 15	Paso 2. Política de Gestión de Datos Personales.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
					164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					individuo de acordar y objetar.	
4	El responsable deberá facilitar al titular medios sencillos y gratuitos para manifestar su consentimiento expreso.	Art. 8	Art. 16	Paso 2. Política de Gestión de Datos Personales.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
					164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.
5	Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.	Art. 9	Art. 56	Paso 2. Política de Gestión de Datos Personales.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.				164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar y objetar.	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.
6	Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 20	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.506 Usos y revelaciones para llevar a cabo el tratamiento, pago, u operaciones de salud.	Disposiciones para usos y revelaciones solamente autorizados con respecto al tratamiento, pago, u operaciones de salud.
					164.508 Usos y revelaciones para las cuales se requiere autorización.	Disposiciones para usos y revelaciones solamente autorizados de información de salud.
					164.510 Usos y revelaciones que requieren una oportunidad para el individuo de acordar	Disposiciones para usos y revelaciones siempre y cuando el individuo haya otorgado su consentimiento.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					y objetar.	
INFORMACIÓN						
7	A través del aviso de privacidad, el responsable tendrá la obligación de informar a los titulares, los datos que recaba, las finalidades necesarias y las que no lo son para la relación jurídica, así como las características principales de su tratamiento. Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Si obtiene los datos de manera automática, deberá informar al titular sobre el uso de estas tecnologías y la forma en que podrá deshabilitarlas.	Art. 15	Art. 14 Art. 23 Art. 112	Paso 2. Política de Gestión de Datos Personales.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
8	Cuando los datos personales sean obtenidos directamente del titular, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.	Art. 3, I Art. 17	Art. 27	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
9	El aviso de privacidad debe contener un mecanismo, para que el titular pueda manifestar su negativa al tratamiento de sus datos personales. Cuando los datos se obtengan de manera indirecta del titular, el responsable deberá darle a conocer el aviso de privacidad y sus cambios.	Art. 18	Art. 14 Art. 29 Art. 32	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
10	Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.		Art. 31	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
CALIDAD						
11	El responsable procurará que los datos personales contenidos en las bases de datos sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.	Art. 11	Art. 36	Paso 2. Política de Gestión de Datos Personales.	164.312(b) Controles de auditoría.	Mecanismos para registrar y examinar los sistemas que contienen información de salud.
					164.312(c)(1) Integridad.	Políticas y procedimientos para proteger la integridad información electrónica de salud.
					164.312(e)(1) Seguridad en la transmisión.	Medidas técnicas para la protección de la información de salud transmitida por la red.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
12	Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo bloqueo de los mismos. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.	Art. 3 III Art. 11	Art. 37	Paso 2. Política de Gestión de Datos Personales.	164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
13	El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales.		Art. 38	Paso 2. Política de Gestión de Datos Personales.	164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
14	Al responsable le corresponde demostrar que los datos personales se conservan, o en su caso, bloquean, suprimen o cancelan.		Art. 39	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.310(d)(2)(i) Eliminación.	Políticas y procedimientos para la eliminación segura de información de salud en donde se encuentre almacenada.
FINALIDAD						
15	El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto al establecido, deberá obtener nuevamente el consentimiento del titular. El titular podrá oponerse o revocar su consentimiento para las finalidades distintas a las que dieron origen a la relación jurídica, sin que ello tenga como consecuencia la conclusión del tratamiento.	Art. 12	Art. 40 Art. 42 Art. 43	Paso 2. Política de Gestión de Datos Personales.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
PROPORCIONALIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
16	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 limitar el periodo de tratamiento al mínimo indispensable.	Art. 13	Art. 45 Art. 46	Paso 2. Política de Gestión de Datos Personales.	164.520 Prácticas para el aviso de privacidad para información de salud protegida.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
CONFIDENCIALIDAD						
17	El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.	Art. 21	Art. 9	Paso 2. Política de Gestión de Datos Personales.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
RESPONSABILIDAD						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
18	El responsable tiene la obligación de velar y responder por el tratamiento de los datos personales en su posesión, debiendo adoptar las medidas necesarias. 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.	Art. 14	Art. 47	Paso 2. Política de Gestión de Datos Personales.	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
19	Los responsables deberán adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Art. 14	Art. 48	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
20	Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización.		Art. 48 - I	Paso 2. Política de Gestión de Datos Personales.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
					164.308(a)(1)(ii)(C) Política de sanción.	Aplicación de sanciones a quienes caen en incumplimiento con las políticas y procedimientos de seguridad.
21	Poner en práctica un programa de capacitación, actualización, y concientización del personal sobre las obligaciones en materia de protección de datos personales.		Art. 48 - II	Paso 9. Mejora Continua y Capacitación. Capacitación.	164.308(a)(5)(i) Entrenamiento y concientización de seguridad.	Implementación de un programa de entrenamiento y concientización de seguridad a todos los niveles de la organización.
22	Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.		Art. 48 - III	Paso 8. Revisiones y Auditoría.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
23	Destinar recursos para la instrumentación de los programas y políticas de privacidad.		Art. 48 - IV	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
24	Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.		Art. 48 - V	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
25	Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.		Art. 48 - VI	Paso 8. Revisiones y Auditoría.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
26	Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.		Art. 48 - VII	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
					164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.
27	Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.		Art. 48 - VIII	Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales.	164.308(a)(1)(ii)(C) Política de sanción.	Aplicación de sanciones a quienes caen en incumplimiento con las políticas y procedimientos de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
28	Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y su Reglamento.		Art. 48 - IX	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
					164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
					164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.
29	Establecer medidas para la trazabilidad de los datos personales, es decir acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.		Art. 48 - X	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.524 Acceso de individuos a información de salud protegida.	Disposiciones para otorgar el acceso a las personas a su información de salud.
					164.526 Corrección de información de salud protegida.	Disposiciones para que las personas requieran la corrección de su información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
30	Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley. Asimismo fomentará la protección de datos personales al interior de la organización.	Art. 30		Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(a)(2) Asignación de la responsabilidad de seguridad.	Asignación de oficial de seguridad responsable del desarrollo e implementación de políticas y procedimientos de seguridad.
SEGURIDAD						
31	Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. No adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Cuando el encargado se encuentre ubicado en territorio mexicano, le serán aplicables las	Art. 19	Art. 4 Art. 9 Art. 57	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la implementación de avisos de privacidad para la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III de Reglamento.					
32	El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	Art. 19	Art. 60	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(D) Revisión de la actividad del sistema de información.	Procedimientos para la revisión de registros de sistemas de información que contienen información de salud.
					164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
33	Elaborar un inventario de datos personales y de los sistemas de tratamiento.		Art. 61 - I	Paso 4. Elaborar un Inventario de Datos Personales.	164.310(d)(1) Controles en dispositivos y medios.	Políticas y procedimientos para la recepción y remoción de dispositivos y medios con información de salud.
					164.316(b)(1) Documentación.	Documentación de políticas y procedimientos para la protección de información de salud.
34	Determinar las funciones y obligaciones de las personas que traten datos personales.		Art. 61 - II	Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.	164.308(a)(3)(ii)(A) Autorización y/o supervisión.	Procedimientos para la autorización y/o supervisión de empleados que acceden a información de salud.
35	Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales.		Art. 61 - III	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
36	Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva.		Art. 61 - IV	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
37	Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.		Art. 61 - V	Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
38	Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.		Art. 61 - VI	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.	164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
39	Llevar a cabo revisiones o auditorías.		Art. 61 - VII	Paso 8. Revisiones y Auditoría.	164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
					164.316(b)(2)(iii) Actualizaciones.	Actualización periódica de la documentación ante cambios que afectan la seguridad de la información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
40	Capacitar al personal que efectúe el tratamiento de datos personales.		Art. 61 - VIII	Paso 9. Mejora Continua y Capacitación. Capacitación.	164.308(a)(5)(i) Entrenamiento y concientización de seguridad.	Implementación de un programa de entrenamiento y concientización de seguridad a todos los niveles de la organización.
41	Realizar un registro de los medios de almacenamiento de los datos personales.		Art. 61 - IX	Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.	164.310(d)(1) Controles en dispositivos y medios.	Políticas y procedimientos para la recepción y remoción de dispositivos y medios con información de salud.
					164.316(b)(1) Documentación.	Documentación de políticas y procedimientos para la protección de información de salud.
42	Contar con una relación de las medidas de seguridad.		Art. 61	3. Acciones a implementar para la seguridad de los datos personales documentadas.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
					164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
					164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
						de salud.
43	Actualizar las medidas de seguridad cuando: I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable. II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 de su Reglamento. IV. Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.		Art. 62	Paso 8. Revisiones y Auditoría.	164.308(a)(1)(ii)(A) Evaluación del riesgo.	Disposiciones para llevar a cabo la evaluación del riesgo sobre la información de salud.
					164.308(a)(1)(ii)(B) Gestión del riesgo.	Disposiciones para la gestión del riesgo sobre la información de salud.
					164.308(a)(8) Evaluación.	Ejecución periódica de una evaluación técnica y no técnica para la evaluación de la seguridad de la información de salud.
VULNERACIONES A LA SEGURIDAD						
44	Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de	Art. 20	Art. 63 Art. 64	Paso 8. Revisiones y Auditoría.	164.308(a)(6)(i) Procedimientos de	Políticas y procedimientos para el manejo de incidentes de

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.			Vulneraciones a la Seguridad de la Información.	incidentes de seguridad.	seguridad.
					164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
					164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
45	En caso de que ocurra una vulneración a la seguridad de los datos personales, el responsable deberá informar al titular al menos lo siguiente: I. La naturaleza del incidente. II. Los datos personales comprometidos. III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para		Art. 65	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
					164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	proteger sus intereses. IV. Las acciones correctivas realizadas de forma inmediata. V. Los medios donde puede obtener más información al respecto.				164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
46	En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.		Art. 66	Paso 8. Revisiones y Auditoría. Vulneraciones a la Seguridad de la Información.	164.308(a)(6)(i) Procedimientos de incidentes de seguridad.	Políticas y procedimientos para el manejo de incidentes de seguridad.
					164.308(a)(6)(ii) Respuesta y reporte.	Actividades para identificar y responder a incidentes de seguridad.
					164.314(b)(2)(iv) Reporte de incidentes de seguridad.	Actividades para el reporte de incidentes de seguridad.
ENCARGADO						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
47	El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable: I. Tratar únicamente los datos personales conforme a las instrucciones del responsable. II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable. III. Implementar las medidas de seguridad conforme a la Ley, su Reglamento y las demás disposiciones aplicables. IV. Guardar confidencialidad respecto de los datos personales tratados. V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales. VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad		Art. 50	1. Recomendación General.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
					164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.
					164.310 Salvaguardas físicas.	Conjunto de controles físicos para la protección de información de salud.
					164.312 Salvaguardas técnicas.	Conjunto de controles técnicos para la protección de información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	competente.					
SUBCONTRATACIONES						
48	La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido.		Art. 51	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
49	Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido. En caso de que la subcontratación no haya sido prevista en cláusulas contractuales, el encargado deberá obtener la autorización correspondiente del responsable previamente. La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.		Art. 54 Art. 55	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
CÓMPUTO EN LA NUBE						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
50	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y su Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se		Art. 52 - I	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.				164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
51	Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cuente con mecanismos, al menos, para:		Art. 52 - II	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de	164.308(a)(1)(i) Proceso de gestión de la seguridad.	Implementación de políticas y procedimientos para prevenir, detectar, contener y corregir violaciones a la seguridad.
					164.308 Salvaguardas administrativas.	Conjunto de controles administrativos para la protección de información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
	a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.			Seguridad.	164.310 Salvaguardas físicas. 164.312 Salvaguardas técnicas.	Conjunto de controles físicos para la protección de información de salud. Conjunto de controles técnicos para la protección de información de salud.
TRANSFERENCIAS						

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
52	Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.	Art. 36	Art. 68 Art. 71 Art. 72 Art. 74	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.
53	Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realiza conforme a lo que establece la Ley y su Reglamento, la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.		Art. 69	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para otorgar el acceso a las personas a su información de salud.
					164.308(b)(4) Contrato escrito.	Disposiciones para que las personas requieran la corrección de su información de salud.

N°	Requerimiento normativo	Referencia LFPDPPP	Referencia Reglamento	Referencia Recomendaciones	Identificador y nombre Objetivo de Control	Descripción
54	En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, su Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, su Reglamento y demás normativa aplicable.		Art. 70	1. Recomendación General	Parte 164 Seguridad y Privacidad.	Provisiones generales, estándares de seguridad para la protección de información electrónica de salud, notificación en caso de vulneración a la seguridad de información de salud, privacidad de información de salud identificable a la persona.
55	La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.		Art. 73 Art. 75	Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. Cumplimiento Cotidiano de Medidas de Seguridad.	164.308(b)(1) Contratos con socios y asociados de negocio y otros acuerdos.	Disposiciones para el establecimiento de contratos y acuerdos con socios y asociados de negocio.
					164.308(b)(4) Contrato escrito.	Disposiciones para la celebración de un contrato escrito con los asociados de negocio.