

POLÍTICA Y PROCEDIMIENTO	
N.º de la política y TÍTULO: HPA07: Informar y mitigar sospechas de infracciones e incidentes de privacidad y seguridad	
Responsable primario de la política: Cumplimiento	N.º DE POLÍTICA: HPA07
Responsable afectado o secundario de la política: Marque los departamentos a cargo del cumplimiento de la política o procedimiento descritos. (Puede ser de manera total o parcial).	
1) <input checked="" type="checkbox"/> Todos los departamentos 2) <input type="checkbox"/> Contabilidad y Finanzas 3) <input type="checkbox"/> Administración 4) <input type="checkbox"/> Manejo del Cuidado 5) <input type="checkbox"/> Reclamos 6) <input type="checkbox"/> Mercado de la Comunidad y Participación de los Miembros 7) <input type="checkbox"/> Cumplimiento 8) <input type="checkbox"/> Configuración 9) <input type="checkbox"/> Cultura y Lingüística 10) <input type="checkbox"/> Servicio al Cliente	11) <input type="checkbox"/> Centros 12) <input type="checkbox"/> Control de Calidad 13) <input type="checkbox"/> Recursos Humanos 14) <input type="checkbox"/> Tecnología de la Información/Sistemas Principales 15) <input type="checkbox"/> Farmacia 16) <input type="checkbox"/> Manejo de Proyectos 17) <input type="checkbox"/> Contratación de Proveedores 18) <input type="checkbox"/> Servicios a Proveedores 19) <input type="checkbox"/> Gestión de Calidad 20) <input type="checkbox"/> Administración de Utilización/Salud del Comportamiento
TIPO DE PRODUCTO: <input checked="" type="checkbox"/> Medi-Cal	Reemplaza a la política n.º: HPA08

I. PROPÓSITO

Resumir los procesos de informe y mitigación para manejar incidentes de privacidad o seguridad, infracciones respecto de la información de salud protegida o información personal (PHI/PII) u otros accesos, usos o divulgaciones no autorizados de PHI o PII.

II. POLÍTICA

- A. La Comisión de Salud del condado de San Joaquin (“Comisión”), que opera como Health Plan of San Joaquin and Mountain Valley Health Plan (“Plan de Salud”), debe informar de inmediato los incidentes de privacidad o seguridad presuntos o confirmados, las infracciones respecto de la PHI o PII y otros accesos, usos o divulgaciones no autorizados de la PHI o PII (en conjunto “incidentes de la ley HIPAA”) a los organismos reguladores según lo requieren las normas de notificación sobre privacidad, seguridad e infracciones de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), las secciones 160 y 164 del título 45 de Código de Regulaciones Federales (CFR), la sección 1798.29 del Código Civil de California y los requisitos contractuales o regulatorios.
- B. El ejecutivo de privacidad (o quien este designe) o el ejecutivo de seguridad informática debe informar los incidentes de la ley HIPAA al Consejo de Supervisión de Seguridad y Privacidad y a las agencias federales y estatales pertinentes.
- C. Las siguientes son maneras de informar un incidente: A través del enlace de SharePoint; contactando a supervisores, gerentes, el equipo ejecutivo o los miembros del equipo de cumplimiento; por fax, correo electrónico o teléfono; de manera anónima o usando los buzones para denuncias de cumplimiento en el lugar de trabajo.
- D. El Plan de Salud debe brindar informes escritos de incidentes de la ley HIPAA sin trabas al Departamento de Servicios de Cuidado de la Salud (DHCS) conforme a esta política.
- E. El Plan de Salud informará las sospechas de incidentes de la ley HIPAA al DHCS usando el portal de dicho departamento. El Plan de Salud informará a los miembros individuales a cuya PHI o PII se haya tenido acceso, o cuya PHI o PII haya sido adquirida, usada o divulgada, o si se presumen estas situaciones, como resultado de una infracción, según lo determina el DHCS.
- F. El Plan de Salud no debe exigir a las personas renunciar a sus derechos como condición para recibir tratamientos, pagos, inscripción en un plan de salud o elegibilidad para los beneficios¹.
- G. El Plan de Salud debe demorar la notificación si un funcionario encargado de hacer cumplir la ley manifiesta que la notificación, el aviso o la publicación impediría una investigación penal o causaría daño a la seguridad nacional².

¹ Sección 164.530(h) del título 45 del CFR.

² Sección 164.412 del título 45 del CFR.

- H. La Unidad de Integridad del Programa del Plan de Salud se encarga de controlar y ejecutar esta política bajo la supervisión del ejecutivo de privacidad y del ejecutivo de seguridad.
- I. El ejecutivo de cumplimiento y el asesor de supervisión de la privacidad revisa esta política al menos una vez al año y la modifica según sea necesario.

III. PROCEDIMIENTO

A. Descubrimiento

Una infracción se debe tratar como si se hubiera descubierto a partir del primer día en el que se sospecha o comprueba; o si, aplicando esmero razonable, una persona (que no sea el infractor) podría tomar conocimiento de ella. Esta persona debe ser un miembro del personal u otro agente del Plan de Salud.

- 1. El personal del Plan de Salud debe informar cualquier incidente de la ley HIPAA de inmediato después de descubrirlo, a través de los siguientes métodos:
 - a. Informar directamente a través del enlace de SharePoint, la aplicación para informes en línea que conecta con el sitio <https://secure.compliance360.com>.
 - b. Informar directamente al supervisor, al gerente o a un miembro del equipo ejecutivo del personal.
 - c. Informar directamente al ejecutivo de privacidad o al ejecutivo de seguridad del Plan de Salud.
 - d. Informar directamente a cualquier miembro del equipo de Administración de Cumplimiento.
 - e. Informar por correo electrónico a PIU@HPSJ.com.
 - f. Informar por fax al (209) 762-4721.
 - g. Informar a través de la aplicación para denuncias anónimas en línea, [Syntrio: Lighthouse Reporting](#).
 - h. Informar usando los buzones para denuncias de cumplimiento ubicados dentro de las instalaciones del Plan de Salud.
 - i. Informar a través de la línea directa de cumplimiento: 1-800-822-6222.
 - j. Miembros del equipo de Administración.

2. Los departamentos y el personal del Plan de Salud informarán de inmediato al Departamento de Cumplimiento usando uno de los métodos descritos antes, cuando descubran un incidente o una infracción presuntos de privacidad o seguridad. No informar constituirá una violación de las políticas y procedimientos.
3. El personal del Plan de Salud está obligado a trabajar con el Departamento de Cumplimiento para investigar y remediar los incidentes de la ley HIPAA si se lo solicita y cumplir con los siguientes requisitos:
 - a. Respetar los procesos y plazos descritos en el acuerdo de nivel de servicio: *Requisitos de corrección de incidentes de privacidad* durante el período de investigación.
 - b. Respetar los roles y las responsabilidades de corrección descritas en el procedimiento de escritorio de cumplimiento y el proceso de corrección de incidentes de privacidad para dueños de negocios.
 - c. La falta de cumplimiento puede dar lugar a la aplicación de medidas disciplinarias conforme a la política HPA09: *Sanciones para el personal de HPSJ*.
4. Los proveedores, contratistas, las personas subcontratadas y sus intermediarios, incluidos los asociados comerciales (en conjunto "Terceros") deben informar sin demora:
 - a. A través de una notificación por correo electrónico a incidentes@dhcs.ca.gov. El tercero está obligado a enviar el mismo mensaje de correo electrónico con copia a la Unidad de Integridad del Programa del Plan de Salud (piu@hpsj.com).
 - b. Por teléfono al (866) 866-0602.
 - c. Cuando el informe se hace a través del portal o por teléfono, el tercero está obligado a enviar una comunicación inmediata que contenga la misma información relacionada con el incidente a la dirección de correo electrónico de la Unidad de Integridad del Programa del Plan de Salud (piu@hpsj.com).

5. Requisito de informar para terceros.
 - a. Se incluyen más detalles sobre las obligaciones de informar para terceros en la política HPA05: *Asociados comerciales*.
 - b. El Plan de Salud brinda información sobre las obligaciones de informar para terceros, según se describe en el *Acuerdo de asociados comerciales*.
 - c. El Plan de Salud informará al DHCS en nombre del tercero, en un plazo de 24 horas desde que toma conocimiento del incidente, en caso de que el tercero no lo haga de forma oportuna.
 - d. El Plan de Salud también cumplirá con los requisitos de informar subsiguientes en caso de que el tercero no cumpla con dichos requisitos.
 - e. Si el tercero no cumple con los requisitos de informar regulatorios, según se describe en el *Acuerdo de asociados comerciales*, esto puede dar lugar a acciones evaluadas por el Plan de Salud que pueden incluir la terminación del contrato.
- B. Informe del Plan de Salud a los miembros.
 1. Un miembro puede presentar una queja sobre violación de la HIPAA al representante de Servicio al Cliente por teléfono o por correo postal. En el *Aviso de Prácticas de Privacidad*, se brindan la dirección y el número de teléfono. Además, puede presentarla a través del sitio web público, [Syntrio: Lighthouse Reporting](#).
 2. El Plan de Salud procesará las quejas de la misma forma que se describe en esta política.
- C. Información de los incidentes de la ley HIPAA a los organismos reguladores.
 1. El Departamento de Cumplimiento del Plan de Salud debe investigar e informar el descubrimiento de incidentes de la ley HIPAA de conformidad con las siguientes pautas:
 2. Infracción:
 - a. El Departamento de Cumplimiento debe notificar al DHCS **de inmediato** a través del portal del DHCS cuando se descubra una infracción de seguridad relacionada con la PHI o PII de forma electrónica si una persona no autorizada adquirió, o se presume que adquirió, la PHI o PII. O bien, debe informar cuando se descubra un incidente de privacidad o seguridad presunto que involucre datos que la Administración del Seguro Social le brindó al DHCS.

- b. Notificar al gerente de contrato, al ejecutivo de privacidad y al ejecutivo de seguridad de la información del DHCS usando la plantilla de Informe de incidentes de privacidad del DHCS.
3. Sospecha de incidente de la ley HIPAA:
 - a. Notificar, **en un plazo de 24 horas**, a través del portal del DHCS cualquier sospecha de incidente de privacidad o seguridad, intrusión o acceso no autorizado, uso o divulgación de PHI o PII que infrinja el contrato del DHCS para 2024 entre el Plan de salud y dicho departamento.
4. Investigación:
 - a. Cuando se descubra un incidente de la ley HIPAA, el Departamento de Cumplimiento iniciará una investigación de inmediato.
 - b. Enviará actualizaciones de la investigación a través del portal del DHCS dentro de las **72 horas** del descubrimiento.
 - c. Presentará los detalles completos de la investigación de incidentes de privacidad a través del portal del DHCS dentro de los **diez (10) días laborales, hábiles** del descubrimiento de la infracción o el uso o la divulgación no autorizados. Si se necesita más tiempo para completar la investigación, el Plan de Salud solicitará una extensión al DHCS y, durante el período de extensión, enviará actualizaciones semanales al DHCS hasta finalizar la investigación. Cuando se descubra un incidente de la ley HIPAA, el Plan de Salud debe hacer lo siguiente:
 - i. Aplicar medidas correctivas sin demora para mitigar cualquier riesgo o daño ocasionado por la infracción y para proteger el entorno operativo.
 - ii. Toda acción relativa a este tipo de divulgaciones no autorizadas es exigida por las leyes y regulaciones federales y estatales aplicables.

5. Notificación al miembro:
 - a. El Plan de Salud debe notificar a cada persona a cuya PHI se haya tenido acceso, o cuya PHI haya sido adquirida, usada o divulgada, o si se presumen de manera razonable estas situaciones, como resultado de dicha infracción.
 - b. Las notificaciones se deben hacer sin demoras injustificadas y en ningún caso después de 60 días calendario posteriores al descubrimiento de una infracción.
 - c. El DHCS debe revisar y aprobar el contenido de la notificación.
 6. Notificación en medios de comunicación:
 - a. Se requiere la notificación en medios de comunicación para infracciones por PHI no protegida que involucran a más de quinientas (500) personas.
 - b. Las notificaciones en los medios de comunicación se deben hacer sin demoras injustificadas y en ningún caso después de 60 días calendario posteriores al descubrimiento de una infracción.
 7. Notificación al secretario del Departamento de Salud y Servicios Humanos (DHHS), Oficina de Derechos Civiles:
 - a. Se requiere la notificación al secretario del DHHS para infracciones por PHI no protegida que involucren a más de quinientas (500) personas.
 - b. Para las infracciones por PHI no protegida que involucran a menos de quinientas (500) personas, el Plan de Salud debe mantener un registro u otra documentación de las infracciones y presentarlos al secretario del DHHS a más tardar sesenta (60) días después del final de cada año calendario.
- D. Cómo determinar qué incidentes de la ley HIPAA se deben informar al DHCS y cuáles no.
1. Todas las infracciones confirmadas de manera razonable se deben informar al DHCS. No obstante, no todos los incidentes de la ley HIPAA son infracciones. Existen tres excepciones:
 - a. Adquisición, acceso o uso no intencional.
 - b. La divulgación involuntaria a una persona autorizada.
 - c. La imposibilidad de retener la PHI.

- d. El *Diagrama para tomar decisiones sobre informes de incidentes de privacidad de HPSJ* es una pauta para determinar qué incidentes de privacidad o seguridad se deben informar al DHCS y cuáles no.
- E. Demora en el cumplimiento de la ley.
1. Si un funcionario encargado de hacer cumplir la ley le manifiesta al Plan de Salud que una notificación, un aviso o una publicación requeridos impediría una investigación penal o causaría daño a la seguridad nacional, el Plan de Salud debe hacer lo siguiente:
 - a. Si la declaración es por escrito y se especifica el plazo de la demora que se requiere, demorará dicha notificación, aviso o publicación por el período especificado por el funcionario.
 - b. Si la declaración es verbal, el Plan de Salud documentará la declaración, incluyendo la identidad del funcionario que la enunció, y demorará la notificación, el aviso o la publicación de forma temporal y por no más de 30 días desde la fecha de la declaración verbal³.

IV. DOCUMENTOS ADJUNTOS

- A. Procedimiento de escritorio: *Cumplimiento y proceso de corrección de incidentes de privacidad para dueños de negocios*
- B. Definiciones de los Planes de Cuidado Controlado de Medi-Cal del Departamento de Servicios de Cuidado Médico (anexo A, documento adjunto I, 1.0 Definiciones)
- C. *Informe de incidentes de privacidad* del DHCS
- D. [Enlace al glosario](#)
- E. Lista de acrónimos usados en los contratos de Cuidado Controlado de Medi-Cal (anexo A, documento adjunto I, 2.0 Acrónimos)
- F. Acuerdo de nivel de servicio: *Requisitos de corrección de incidentes de privacidad*

³ Sección 164.412 del título 45 del CFR.

V. REFERENCIAS

- A. Secciones 160, 162 y 164.412 del título 45 de Código de Regulaciones Federales (CFR).
- B. Secciones 56 y 56.37 del Código Civil de California: Ley de Confidencialidad de la Información Médica.
- C. CMP01: *Respuesta a las violaciones de cumplimiento y cómo prevenirlas.*
- D. CMP DP009: *Recepción e informe de incidentes de privacidad.*
- E. Anexo G del contrato del DHCS.
- F. HPA01: *Consejo de Supervisión de Seguridad y Privacidad.*
- G. HPA09: *Sanciones para el personal de HPSJ.*
- H. *Acuerdo de asociados comerciales de HPSJ.*
- I. *Diagrama para tomar decisiones sobre informes de incidentes de privacidad de HPSJ.*
- J. *Aviso de prácticas de privacidad de Medi-Cal.*
- K. Preguntas frecuentes sobre incidentes de privacidad.
- L. Acuerdo de nivel de servicio: *Requisitos de corrección de incidentes de privacidad.*

VI. HISTORIAL DE REVISIÓN

* Versión 001 vigente desde 01/01/2023

Versión*	Resumen de la revisión	Fecha
000	03/03, 07/03, 04/05, 01/09, 05/09, 06/12, 09/14, 11/18, 06/20, 07/20, 12/20, 2/21, 11/21, 10/22, 12/22, 2/23	No disponible.
001	Se cambió la política HPA07 a la nueva plantilla para 2023.	03/21/2023
002	Se agregó información sobre el acuerdo de nivel de servicio: <i>Requisitos de corrección de incidentes de privacidad</i> en la sección B. "Informe de incidentes o infracciones de privacidad o seguridad a HPSJ".	05/23/2023
003	Se revisó el procedimiento para que los asociados comerciales informen infracciones.	07/14/2023

Versión*	Resumen de la revisión	Fecha
004	Según el contrato del DHCS para 2024, se agregó contenido a la política sobre asociados comerciales que mitigan infracciones e incidentes de seguridad.	08/30/2023
005	Se dio formato al contenido por motivos de legibilidad.	09/21/2023
Fecha de vigencia inicial: 04/14/2003		

VII. REVISIÓN Y APROBACIÓN DEL COMITÉ

Nombre del comité	Versión	Fecha
Comité de Cumplimiento	005	12/7/2023
<ul style="list-style-type: none"> Consejo de Supervisión de Seguridad y Privacidad 	005	11/7/2023
<ul style="list-style-type: none"> Comité de Integridad del Programa 		
<ul style="list-style-type: none"> Comité de Auditorías y Supervisión 		
<ul style="list-style-type: none"> Comité de Revisión de Políticas 	005	11/15/2023
Comité de Administración de Utilización y Calidad		
<ul style="list-style-type: none"> Comité de Calidad de la atención 		
<ul style="list-style-type: none"> Comité de Quejas Formales 		

VIII. APROBACIÓN DE AGENCIAS DE REGULACIÓN

Departamento	Revisor	Versión	Fecha
Departamento de Servicios de Cuidado Médico	No disponible.	No disponible.	No disponible.
Departamento de Cuidado Médico Controlado	No disponible.	No disponible.	No disponible.



IX. FIRMAS DE APROBACIÓN

Firma	Nombre del cargo	Fecha
	Presidente, Comité de Revisión y Acreditación de Pares	
	Responsable de la política	
	Ejecutivo del departamento	
	Director ejecutivo	

* Las firmas se archivan; no estarán en la copia publicada.