| **POLÍTICA Y PROCEDIMIENTO** | |
|---|---|
| **TÍTULO:**<br>Resguardo de información de salud protegida e información que permite identificar | |
| **TITULAR DE LA POLÍTICA DEL DEPARTAMENTO:**<br>Cumplimiento | **N.º DE POLÍTICA:** HPA42 |
| **DEPARTAMENTO AFECTADO:**<br>Marque todos los departamentos afectados | |
| ☐ Administración<br>☐ Reclamos<br>☐ Cumplimiento<br>☐ Servicio al Cliente<br>☐ Asuntos Exteriores<br>☐ Centros<br>☐ Finanzas | ☐ Recursos Humanos<br>☐ Tecnología de la Información<br>☐ Mercadeo<br>☐ Administración Médica<br>☐ Redes de Proveedores<br>☐ Manejo de Proyectos<br>☒ TODOS |
| **FECHA DE ENTRADA EN VIGENCIA:**<br>15/5/19 | **FECHA DE REVISIÓN/MODIFICACIÓN:**<br>4/19, 12/20, 4/21 |
| **FECHA DE APROBACIÓN DEL COMITÉ:**<br>PRC: 5/19, 7/20, 4/21<br>Comité de Cumplimiento: 7/19 | **FECHA DE RETIRO:** |

| **TIPO DE PRODUCTO:** | **REEMPLAZA:** |
|---|---|
| Medi-Cal | IT15: *Protección de las áreas de trabajo y el acceso electrónico*. IT18: *Procedimiento de la aplicación de registro*. IT21: *Controles de dispositivos y medios.* IT22: *Mantenimiento de la integridad y seguridad de información de salud protegida en formato electrónico*. IT33: *Uso del correo electrónico*. IT34: *Supervisión de sistemas y revisión de actividades.* IT203: *Resguardo de información de salud protegida en formato electrónico.* HPA06: *Resguardos administrativos para información de salud protegida.* HPA26: *Uso y divulgación de información de salud protegida.* HPA27: *Divulgación en los procedimientos judiciales.* HPA28: *Divulgación para fines de cumplimiento de la ley.* HPA29: *Divulgación para funciones especializadas del Gobierno.* HPA30: *Divulgación para actividades de supervisión de salud.* HPA31: *Resguardo de información de salud protegida perteneciente a miembros fallecidos o dados de baja.* HPA32: *Divulgación a representantes personales.* HPA33: *Verificación de la identidad para divulgar información de salud protegida.* HPA36: *Divulgación de información de salud protegida del miembro*. HPA38: *Divulgación a compañías* |

| | |
|---|---|
| | *de seguros de indemnización a trabajadores.*<br>HPA39: *Anonimización de la información de salud protegida.* |

## I. PROPÓSITO

Health Plan of San Joaquin/Mountain Valley Health Plan ("HPSJ/MVHP") implementará medidas de resguardo razonables de la información de salud protegida (PHI) en los registros de los miembros contra usos o divulgaciones intencionales o que no están permitida por la norma de seguridad y privacidad de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) ni por la Ley de Confidencialidad de la Información Médica (CMIA). En esta política y procedimiento (P&P) se consideran los controles de privacidad y seguridad implementados para resguardar esta información confidencial.

## II. POLÍTICA

A. En HPSJ/MVHP se implementan medidas de resguardo administrativas, físicas y técnicas que protegen de manera adecuada y razonable la confidencialidad, integridad y disponibilidad de la información de salud protegida y la PHI en formato electrónico que se crean, reciben, guardan, usan o transmiten en nombre del Departamento de Servicios de Atención Médica (DHCS), conforme a las secciones 164.308, 164.310, 164.312 y 164.502(f) del título 45 del Código de Regulaciones Federales, para evitar un uso o divulgación de PHI que no sean los previstos en este acuerdo (Anexo G, disposición C.2 del Contrato del DHCS).

B. En HPSJ/MVHP no se pueden condicionar tratamientos, pagos, inscripciones ni la elegibilidad para recibir beneficios a personas que tengan una autorización, excepto en circunstancias limitadas conforme a la sección 164.508(b)(4) del título 45 del Código de Regulaciones Federales (CFR).

C. En HPSJ/MVHP se controlará el acceso a la PHI y se garantizará un manejo apropiado. Las violaciones a esta política deberán informarse al Departamento de Cumplimiento, ya sea en persona, por correo electrónico o de manera anónima según se describe en la P&P número CMP01: *Respuesta a las violaciones de cumplimiento y cómo prevenirlas.*

D. En HPSJ/MVHP pueden divulgar información protegida de salud al familiar de un miembro fallecido que haya participado en la atención médica o pagado el cuidado médico antes de la muerte del miembro, siempre que la PHI sea relevante respecto a la participación de esa persona y no vaya en contra de una preferencia previa expresada por el miembro y conocida por la entidad cubierta.

E. Los miembros tienen derecho a anular una autorización, siempre que se haga por escrito, excepto en la medida en que HPSJ/MVHP ya haya actuado conforme a ella.

F. En HPSJ/MVHP cumplirán los siguientes términos del contrato del Departamento de Servicios de Atención Médica (DHCS): "Usar y divulgar PHI solo para llevar adelante las funciones, actividades o los servicios especificados en este acuerdo para el DHCS, o en su nombre, siempre que esos usos y divulgaciones no violen las regulaciones de la ley HIPAA" (Anexo G.III.A del Contrato del DHCS).

G. El jefe de cumplimiento tiene la responsabilidad de garantizar que las divulgaciones de PHI que no sean de rutina, incluidos servicios sensibles, estén permitidas y sean necesarias. El personal de atención de salud con licencia de HPSJ/MVHP está al tanto de las actividades en las que se permite divulgar información de salud protegida sin permiso del miembro conforme a la ley HIPAA.

H. Comunicaciones y transmisiones electrónicas

1. El equipo de trabajo debe encriptar los mensajes de correo electrónico que contengan información confidencial antes de enviarlos.
2. El equipo de trabajo debe usar un túnel encriptado, una red privada virtual (VPN) o protocolos, como la transferencia segura de archivos (SFTP) o el número de servidores seguros (SSL) cuando transmita información confidencian en una red pública (por ejemplo, internet).

I. Almacenamiento y medios electrónicos

1. En HPSJ/MVHP está prohibido guardar información de salud protegida, incluida la PHI en formato electrónico, en los discos duros locales.
2. En HPSJ/MVHP se debe encriptar la PHI en formato electrónico guardada en medios y dispositivos portátiles (como computadoras portátiles, almacenamientos portátiles y casetes).
3. En HPSJ/MVHP se deben encriptar los discos duros que contengan PHI en formato electrónico si el cifrado es apropiado y razonable. En situaciones en las que HPSJ/MVHP determine que el encriptado no es apropiado o razonable, después de haber realizado una cuidadosa evaluación y consideración, deberán implementar una forma alternativa de protección en HPSJ/MVHP que ofrezca el mismo nivel de resguardo que el cifrado.
4. En HPSJ/MVHP deberán encargarse del traslado de *hardware*, almacenamiento y medios electrónicos que contengan PHI en formato electrónico.
5. En HPSJ/MVHP deberán borrar los medios electrónicos que contengan PHI en formato electrónico antes de volver a usarlos.
6. En HPSJ/MVHP deberán borrar o destruir físicamente los medios electrónicos que contengan PHI en formato electrónico antes de eliminarlos.

J. Los enfoques y procedimientos de cifrado de HPSJ/MVHP deben usar un algoritmo de encriptación compatible con FIPS 140-2. K. Registro de actividades y controles

1. En HPSJ/MVHP deberán registrar o grabar las actividades de los sistemas informáticos que creen, reciban, guarden o transmitan PHI en formato electrónico.
2. En HPSJ/MVHP deberán examinar periódicamente las actividades y los registros de ingreso de la información en los sistemas informáticos que creen, reciban, mantengan o transmitan PHI en formato electrónico.

L. Computadoras y dispositivos electrónicos

1. Las computadoras y los dispositivos electrónicos que creen, reciban, guarden o transmitan PHI en formato electrónico deben cumplir estos requisitos:

    a. Tener protección contra *software* malintencionado, incluidas las revisiones críticas del sistema operativo, los paquetes de servicio o las actualizaciones de servicios aplicables.
    b. Tener los discos duros encriptados o protegidos con controles equivalentes a la protección que ofrece un cifrado.
    c. Bloquearse automáticamente después de un período de inactividad.
    d. Estar limitados a usuarios y procesos con privilegios mínimos necesarios para llevar adelante sus tareas o funciones.

2. En HPSJ/MVHP deberán realizar el mantenimiento de las computadoras o los dispositivos electrónicos conectados a la red, incluida la aplicación de revisiones críticas de seguridad, dentro de los 30 días a partir de la notificación del proveedor o de seguridad de TI. En HPSJ/MVHP se aplican otras revisiones no designadas como críticas dentro de un programa normal de mantenimiento que podría surgir del anterior.

## III. PROCEDIMIENTO

A. El jefe de cumplimiento (ejecutivo de privacidad) y el ejecutivo de seguridad tendrán la responsabilidad de administrar las protecciones de información de salud protegida y de PHI en formato electrónico.

a. Documentación física que contiene información de salud protegida.
    i. Los documentos que contengan PHI se guardarán en gabinetes cerrados con llave o lugares seguros, en espacios de trabajo.
    ii. Se enviarán por correo en formato seguro, siguiendo los requisitos de rastreo y firma, las grandes cantidades de documentación con información de salud protegida. Esta

información se mantendrá y guardará de acuerdo con lo dispuesto en el programa de
Administración y Retención de Registros.

iii. La destrucción definitiva de la documentación con PHI se lleva adelante conforme a la P&P número CMP02: *Administración y retención de registros*.

b. Comunicaciones orales
   i. Solo se hablará sobre información de salud protegida en las áreas de trabajo apropiadas, no en zonas ni áreas públicas.
   ii. Las entrevistas y conversaciones con los miembros de HPSJ/MVHP se llevarán adelante en áreas seguras (por ejemplo, puede usarse la sala de miembros).

c. Comunicaciones y transmisiones electrónicas
   i. Mensajes electrónicos (correo electrónico)

      1. En HPSJ/MVHP se usan métodos de cifrado (por ejemplo, los botones "Envío seguro" en Outlook de escritorio o "Seguridad" en el Outlook del Office 365 para encriptar los correos electrónicos a destinatarios fuera del dominio de www.hpsj-mvhp.org.

      2. Los usuarios deben abstenerse de incluir PHI en el asunto de un correo electrónico.

      3. El sistema de correo electrónico empresarial revisa y evalúa los mensajes de salida, según un conjunto de criterios para la PHI, y encripta automáticamente los mensajes que no están cifrados para que cumplan con esos criterios.

   ii. En HPSJ/MVHP se usan túneles encriptados o protocolos de seguridad, como VPN, SSL o SFTP para las comunicaciones o transferencias electrónicas de archivos que contengan PHI en formato electrónico a través de redes públicas. Cuando los proveedores o asociados no están equipados para usar el

protocolo SFTP, en HPSJ/MVHP usamos aplicaciones como el programa PGP (privacidad bastante buena) para cifrar los archivos antes de transferirlos mediante un túnel no encriptado.

iii. El equipo de trabajo y los proveedores y asociados de HPSJ/MVHP usan VPN o Citrix en las sesiones remotas interactivas donde se transmite PHI en formato electrónico a través de redes públicas.

iv. Las aplicaciones web usan un número de conexión segura (TLS) para garantizar la autenticación e integridad de la PHI en formato electrónico transmitida por HTTP como HTTPS.

d. Almacenamiento y medios electrónicos

i. En Operaciones de Tecnología de la Información (TI) tienen procedimientos para garantizar que el medio portátil encripte los datos guardados de manera automática.

ii. Cuando es necesario guardar PHI en formato electrónico, los usuarios guardan esta información en discos de la red.

iii. En Operaciones de TI no habilitan puertos USB en computadoras de escritorio.

iv. Los usuarios pueden solicitar poder escribir en el almacenamiento portátil con autorización y de conformidad con esta política.

v. En Operaciones de TI proveen unidades de USB que se encriptan de manera automática a los usuarios autorizados a tener habilitado su puerto USB.

vi. En HPSJ/MVHP se registra la recepción, instalación y destrucción de todos los medios electrónicos que contengan PHI en formato electrónico según se especifica en los estándares y procedimientos de Operaciones de TI.

vii. En HPSJ/MVHP se borran o eliminan de manera segura los medios que contengan PHI en formato electrónico antes de volver a usarlos en otro sistema o por otro usuario, conforme a los estándares y procedimientos de trabajo de Operaciones de TI.

viii. En HPSJ/MVHP se destruyen de manera segura, antes de su eliminación, todos los medios electrónicos que contengan (o que se supone que contienen) PHI en formato electrónico mediante la destrucción física o una limpieza según los estándares y procedimientos de trabajo de Operaciones de TI.

e. Cifrado

i. En HPSJ/MVHP tienen mecanismos para cifrar y descifrar la información cada vez que se considere adecuado.

ii. En HPSJ/MVHP se usan los siguientes factores para evaluar la pertinencia y razonabilidad del cifrado de los datos archivados:

1. La capacidad de la aplicación para funcionar en un servidor con disco encriptado.
2. La capacidad de la aplicación o el servidor para soportar los mecanismos de cifrado o descifrado de datos.
3. El impacto del cifrado en el desempeño y la funcionalidad de la aplicación.
4. El costo de los recursos adicionales para implementar o soportar cifrados.

iii. En situaciones en las que HPSJ/MVHP determine que el cifrado de los datos archivados no es razonable o apropiado, HPSJ/MVHP implementará todos o algunos de los siguientes controles de compensación:

1. Servidores propios en salas de servidores o centros de datos seguros.

2. Registro de todos los accesos a las salas de servidores o centros de datos.
3. Seguimiento de mejores prácticas de seguridad para reforzar los servidores.
4. Sistemas para implementar la detección y prevención de intrusiones (IDS/IPS) o de prevención de pérdida de datos (DLP).

f. Registro de actividades y controles

i. Los sistemas informáticos de HPSJ/MVHP registran actividades, como intentos fallidos de autenticación, cambios en la configuración, proceso de inicio, apagado y reiniciado, y detección de *software* maligno o de actividades sospechosas.

ii. En HPSJ/MVHP hay mecanismos para revisar los registros de accesos no autorizados.

g. Computadoras y dispositivos electrónicos

i. En HPSJ/MVHP se resguardan los recursos informáticos que tienen acceso a información confidencial mediante el uso de dispositivos de seguridad perimetrales, como cortafuegos.

ii. En el departamento de TI distribuyen computadoras con la capacidad para escribir o acceder al almacenamiento portátil sin habilitar.

iii. Las computadoras incluyen un *software* para proteger contra *software* malignos (como programas de antivirus) y mecanismos para instalar nuevas versiones de seguridad y actualizaciones críticas del sistema operativo (OS).

iv. En el departamento de TI tienen políticas y procedimientos para casos de vulnerabilidad y para la gestión de revisiones. El enfoque basado en los riesgos de HPSJ/MVHP para priorizar las

revisiones críticas garantiza la aplicación apropiada y en tiempo y forma de las revisiones vinculadas con las vulnerabilidades de aplicación, sistema y red del dispositivo.

v. Las computadoras y los dispositivos electrónicos que tienen acceso a PHI en formato electrónico automáticamente despliegan un protector de pantalla protegido con contraseña después de los 10 minutos sin actividad (tiempo improductivo).

h. Obtener una autorización del miembro o representante personal

i. Una vez recibida la solicitud según se indica en el anexo III.A., se requiere que los miembros completen una autorización. Pueden presentar la autorización por correo o completarla en una oficina de HPSJ/MVHP. El equipo de trabajo de HPSJ/MVHP puede obtener la autorización a través de Intranet/Forms/HIPAA. Las autorizaciones deben hacerse en documentos separados y no pueden combinarse con ningún otro tipo de formulario.

ii. Las autorizaciones se deben enviar únicamente a la dirección actual del miembro que figura en nuestra base de datos de miembros. Está terminantemente prohibido enviar las autorizaciones a una dirección diferente.

iii. Cuando completen un *Formulario de autorización* en una oficina de HPSJ/MVHP, el miembro del equipo de trabajo de Servicio al Cliente les pedirá a los miembros de HPSJ/MVHP una identificación con foto y documentos que figuren en los registros de llamada.

iv. Los representantes personales de miembros que no sean personas discapacitadas o de la tercera edad deben presentar o mostrar una prueba de su autoridad legal para completar una autorización en nombre del miembro conforme a la política HPA32: *Divulgaciones a representantes personales*. Entre las pruebas válidas se incluyen las siguientes: certificado de nacimiento de un miembro con discapacidad física o mental que demuestre que el representante personal es el padre o la madre; documentos del condado o un tribunal que indiquen que el representante personal tiene permiso para buscar y obtener atención médica para el miembro; un poder que otorgue al representante legal el derecho a actuar en nombre del miembro; o bien una declaración jurada donde el representante personal figure como cuidador.

i. Los miembros con discapacidad o de la tercera edad no necesitan completar un *Formulario de autorización* cuando tengan una incapacidad física o mental. El personal puede usar los datos guardados y presentados por el DHCS para identificar al representante personal. El Departamento de Cumplimiento deberá aprobar todas las demás pruebas.

j. En caso de que HPSJ/MVHP deba obtener una autorización del miembro o su representante personal, el personal de HPSJ/MVHP completará todas las secciones del *Formulario de autorización* antes de dárselo al miembro o su representante personal para que lo firmen.

k. En caso de que HPSJ/MVHP obtenga la autorización del miembro o su representante personal, se entregará al miembro o su representante personal una copia de la autorización firmada. Cuando el miembro o su representante personal quieran obtener la autorización, se les puede brindar una copia si la solicitan.

l. En HPSJ/MVHP pueden divulgar la información de salud protegida de miembros fallecidos en los siguientes casos.

    I. Para miembros fallecidos, si la PHI se solicita dentro de los 50 años de la muerte del miembro, HPSJ/MVHP considerará a los

albaceas, administradores u otra persona que tenga autoridad para actuar en nombre del miembro fallecido en calidad de representante personal. Estos representantes deberán brindar documentos legales que respalden su autoridad legal.

II. Para advertir a las fuerzas de seguridad sobre la muerte de una persona cuando haya una sospecha que la causa de muerte fue consecuencia de una acción criminal.

III. Para llevar investigaciones exclusivamente sobre la PHI de los descendientes.

IV. Para facilitar la donación y el trasplante del órgano, ojo o tejido de organizaciones de obtención de órganos u otras entidades involucradas en la obtención, el trasplante o el banco de órganos, ojos o tejidos de donantes fallecidos.

V. A un miembro de la familia u otra persona que participó en la atención médica o pagó los cuidados médicos de la persona antes de su muerte, a menos que vaya en contra de una preferencia previa expresada por la persona fallecida y de la que HPSJ/MVHP tenga conocimiento.

m. Revisión de las autorizaciones

i. El Departamento de Servicio al Cliente revisará todos los formularios de autorización que se presenten a HPSJ/MVHP antes del uso o la divulgación de la PHI de un miembro, tal como se indica en el *Formulario de autorizació*n.

ii. El Departamento de Cumplimiento revisará todos los formularios de autorización que no sean de HPSJ/MVHP antes del uso o la divulgación de información de salud protegida como se indica en el *Formulario de autorización*. Las autorizaciones se consideran deficientes o nulas en estos casos:

1. La autorización se solicita para divulgar la PHI del miembro para fines no relacionados con la administración del programa Medi-Cal.

2. El representante personal de un menor firmó la autorización, por ejemplo, el padre o la madre, pero la PHI solo se puede usar o divulgar con el permiso del menor, según se define en el Código de Familia del Estado de California.

3. Falta alguno de los datos en el formulario.

4. Se cumplió la fecha de vencimiento o en HPSJ/MVHP se conoce algún hecho que implica su terminación.

5. El miembro anuló más adelante una autorización válida.

6. Hay datos en el *Formulario de autorización* que HPSJ/MVHP sabe que son falsos.

iii. El Departamento de Cumplimiento documentará las restricciones y prohibiciones indicadas por el miembro o su representante personal, incluidos los relacionados con servicios sensibles, en las secciones "Representantes personales" y "Alertas" del módulo del miembro.

n. Anulación de autorizaciones

i. Los miembros o sus representantes personales tienen derecho a dar de baja una autorización en cualquier momento. Se debe pedir la anulación por escrito.

ii. En HPSJ/MVHP harán todo lo necesario para respetar y cumplir con la anulación, a menos que HPSJ/MVHP ya haya tomado medidas como consecuencia de esa autorización.

o. Documentación

i. Se brindará al miembro o a su representante personal una copia del *Formulario de autorización* firmado cuando HPSJ/MVHP pida la autorización.

ii. El Departamento de Cumplimiento mantendrá todos los formularios de autorización válidos o nulos y las anulaciones subsiguientes.

iii. Los formularios de autorización y anulación se conservarán conforme a la política CMP02: *Administración y retención de registros.*

iv. Funciones especializadas del Gobierno.

v. El Departamento de Cumplimiento revisará y responderá las solicitudes.

vi. Las solicitudes aceptadas se limitan a aquellas autorizadas en la sección 164.512(k) del título 45 del CFR.

vii. El Departamento de Cumplimiento pedirá la identificación pertinente para verificar a los funcionarios que soliciten acceso a la PHI del miembro cuando se encuentren en las instalaciones.

viii. El Departamento de Cumplimiento enviará por fax o por correo los materiales en respuesta a los funcionarios en un sobre marcado como "confidencial".

B. **Documentos adjuntos**

A. Enlace del *Glosario de términos*

C. **REFERENCIAS**

a. Secciones 160 y 162 del título 45 del CFR.
b. Sección 164.308 (a)(1)(ii)(D) del título 45 del CFR: Revisión de la actividad del sistema informático.
c. Sección 164.310(d)(1) del título 45 del CFR: Controles de dispositivos y medios.
d. Sección 164.310(d)(2)(i) del título 45 del CFR: Formas de eliminación.

e. Sección 164.310(d)(2)(ii) del título 45 del CFR: Reutilización de medios.
f. Sección 164.310(d)(2)(iii) del título 45 del CFR: Rendición de cuentas.
g. Sección 164.312(b) del título 45 del CFR: Controles de auditoría.
h. Sección 164.312(e)(1) del título 45 del CFR: Seguridad de las transmisiones
i. Sección 164.312(e)(2)(i) del título 45 del CFR: Controles de integridad.
j. Sección 164.312(e)(2)(ii) del título 45 del CFR: Cifrado
k. Sección 164.312(a)(2)(iv) del título 45 del CFR: Cifrado y descifrado.
l. Sección 164.502(f) del título 45 del CFR.
m. Titulo 56 del Código Civil de California (CMIA).
n. CMP01: *Respuesta a las violaciones de cumplimiento y cómo prevenirlas.*
o. CMP02: *Administración y retención de registros.*
p. Plan del Programa de Cumplimiento (auditoría interna y administración de riesgos).
q. Anexo G, disposición C.2 del Contrato del DHCS.
r. FIPS PUB 140-2: Requisitos de seguridad para módulos criptográficos.
s. Ley de Tecnología de la Información de la Salud para la Salud Económica y Clínica (ley HITECH).
t. HPA08: *Mitigación.*
u. HPA33: *Verificación de la identidad.*
v. HR11: *Medidas correctivas.*
w. IT33: *Correos electrónicos.*
x. Publicación especial (SP) de NIST 800-53, revisión 4: *Controles de seguridad y privacidad para sistemas informáticos y organizaciones federales*.

## D. **APROBACIONES DE AGENCIAS DE REGULACIÓN**

Conforme a un acuerdo de HPSJ/MVHP con el Departamento de Servicios de Atención Médica (DHCS), se aprueba la política HPA42 para su implementación debido a que ha estado en revisión durante los últimos 60 días.

E. **HISTORIAL DE REVISIÓN**

| **ESTADO** | **FECHA DE REVISIÓN** | **RESUMEN DE LA REVISIÓN** |
|---|---|---|
| Propuesto | 31/1/19 | Combinación de contenidos de políticas existentes y contenido agregado para ajustarse a la norma de seguridad de la ley HIPAA. |
| Finalizado | 2/4/19 | Aprobado por el Consejo de Supervisión de Seguridad y Privacidad (PSOC) |
| Modificado | 13/1/20 | Se agregó política y procedimientos al glosario. |
| Modificado | 10/2/20 | Se combinaron los resguardos administrativos de la política HPA06 y partes de la política HPA31 sobre protección de PHI de miembros fallecidos a IT203. Se cambió el título de la política, ahora es HPA42 en vez de IT203 y el titular de la política pasó de TI a Cumplimiento. Se incorporaron y actualizaron el propósito, la política y el procedimiento. Se combinaron las referencias. |
| Modificado | 25/2/20 | Se cambiaron formato y título. |
| Modificado | 11/12/20 | Se combinó la política HPA26 en la política HPA42. AG. |
| Modificado | 5/4/21 | Se revisó la política para su precisión. |