CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR CONSUMER INFORMATION & INSURANCE OVERSIGHT

Proteger la información de los consumidores e implementar la práctica de la ciberseguridad

Los agentes y corredores desempeñan un papel fundamental en la protección de la información de identificación personal (IIP) de los consumidores en el Health Insurance Marketplace®. Dado que las brechas de ciberseguridad son una amenaza creciente para las pequeñas empresas, esta hoja de consejos dispone de una guía práctica para que los agentes y corredores implementen la práctica de la ciberseguridad en su trabajo diario.

Consejos para implementar la práctica de la ciberseguridad

La implementación de la ciberseguridad consiste en un conjunto de prácticas que deben realizarse con regularidad para mantener la seguridad de sus dispositivos y redes con el fin de mantener a salvo los datos confidenciales de los clientes y protegerlos de robos y ataques. Estas prácticas incluyen:

- **Copias de seguridad:** Realice copias de seguridad periódicas de los archivos importantes en una ubicación independiente y segura que permanezca a salvo en caso de que se produzca un fallo de ciberseguridad.
- **Concientización y educación**: Aprenda a evitar las estafas de phishing y a prevenir los ataques de malware. Los agentes y corredores también deberían compartir esta información con sus empleados.
- **Cifrado:** Utilice el cifrado para proteger los datos confidenciales en archivos y dispositivos.
- **Higiene de contraseñas:** Mantenga una buena higiene de contraseñas requiriendo contraseñas únicas, empleando gestores de contraseñas, revisando la frecuencia con la que se actualizan las contraseñas y utilizando la autenticación multifactorial (MFA) para dificultar a los hackers el acceso no autorizado. Dado que las contraseñas largas son más seguras, los agentes y corredores deben utilizar contraseñas de entre 8 y 12 caracteres.
- **Gestión de parches:** Mantenga siempre actualizado el software e instalar parches de seguridad tanto en los dispositivos propiedad de la empresa como en los personales utilizados para el trabajo.
- **Software de seguridad**: instale software de seguridad para defender los sistemas contra programas maliciosos como ransomware, spyware, gusanos, rootkits y troyanos. Además, realice análisis periódicos para detectar actividades inusuales.

Buenas prácticas para proteger la información de identificación personal (IIP)

En persona:

- Guarde bajo llave los formularios de consentimiento del consumidor en papel.
- Durante las citas con los consumidores, utilice espacios privados para garantizar la privacidad
- Elimine la IIP de forma coherente con las normas y requisitos de conservación del FFM.

Vía electrónica:

- No envíe ni reenvíe correos electrónicos con información confidencial a cuentas de correo personales.
- No utilice dispositivos móviles no autorizados para acceder a información de identificación personal.
- Almacene la IIP de forma segura en un archivo protegido con contraseña en un ordenador protegido con contraseña al que solamente tengan acceso las personas autorizadas.

En papel:

- Asegúrese de que los originales de los registros de los consumidores se devuelvan antes de que salgan de su oficina y haga solamente copias para usted u otras personas si es necesario para llevar a cabo las tareas requeridas.
- Tenga a mano carpetas de papel manila para entregarlas a los consumidores con sus documentos dentro, para mantenerlos en un solo lugar y proteger el contenido de las miradas de otros.