oscar

Cómo proteger la información de los clientes

Resumen:

Salvaguardar los datos confidenciales es crucial para mantener la confianza, cumplir los requisitos legales y reglamentarios, y mitigar los riesgos asociados a las violaciones de datos. Al dar prioridad a la seguridad de los datos, los agentes de seguros pueden garantizar la confidencialidad, integridad y disponibilidad de la información de los clientes, fomentando una sólida relación cliente-agente. Unas medidas sólidas de protección de datos no solo protegen la información personal identificable de los clientes, sino que también los protegen contra el fraude, el robo de identidad y el acceso no autorizado. Para mantener la privacidad y confidencialidad de los datos de los clientes, es fundamental aplicar medidas de encriptación, almacenamiento seguro de los datos, controles de acceso y auditorías regulares de seguridad.

Qué se considera información sensible del cliente:

Los principales formularios de información sobre clientes en el sector de los seguros incluyen datos personales, información sobre pólizas, historial de reclamos y datos de evaluación de riesgos.

- Los datos personales recogen el nombre, la información de contacto, la edad y la dirección de residencia del cliente, que son esenciales a efectos de identificación y comunicación.
- La información sobre la póliza incluye el tipo de cobertura, los límites de la póliza, los deducibles y los detalles del pago de la prima. El historial de reclamos registra los reclamos anteriores realizados por el cliente, incluida la naturaleza del reclamo, los pagos y cualquier documentación relevante.
- Los datos de evaluación de riesgos implican evaluar el perfil de riesgo del cliente en función de factores como su salud y su estilo de vida. Estos formularios de información ayudan a las aseguradoras en la suscripción, gestión de pólizas y tramitación de reclamos.

Normativas del sector aplicables a la protección de la información:

Estas normativas relacionadas con la atención médica son fundamentales tanto para los agentes como para las compañías de seguros a fin de proteger la información de los clientes, mantener la privacidad y cumplir con las obligaciones legales en el sector de la atención médica.

Normativa	Ejemplo	Descripción
Privacidad de la información de salud	Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA)	Regula la protección de la información relativa a la salud por parte de las compañías de seguros.
Notificación de violación de seguridad	Normas de notificación de infracciones de la HIPAA	Obliga a notificar a las personas y a las autoridades en caso de violación de la información relativa a la salud protegida.
Avisos de privacidad	Normas de privacidad de la HIPAA	Obliga a ofrecer a las personas una notificación de las prácticas de privacidad y de sus derechos en relación con la información relativa a la salud.
Acuerdos de Socios Comerciales (BAA)	Requisitos HIPAA para socios comerciales	Exige acuerdos por escrito con terceros que manejen información relativa a la salud protegida. Todos los agentes firman un acuerdo de asociación comercial al firmar el acuerdo de productor.

Buenas prácticas para el manejo de la información personal identificable (PII):

Tema	Detalles	Ejemplo
Controles de acceso	Implemente fuertes controles de acceso y mecanismos de autenticación de usuarios.	Imponer contraseñas seguras, aplicar controles de acceso basados en funciones y utilizar la autenticación multifactor para acceder a los sistemas con PII.
Almacenamiento seguro de datos	Emplee métodos seguros para almacenar la PII.	Almacenar la PII en bases de datos encriptadas alojadas en servidores seguros con estrictos controles de acceso y parches de seguridad regulares.
Formación de los empleados	Lleve a cabo programas de formación exhaustivos sobre la privacidad y la seguridad de los datos.	Ofrecer sesiones de formación regulares a los empleados sobre el manejo de la PII, el reconocimiento de los intentos de phishing y el seguimiento de los protocolos de seguridad adecuados.
Plan de respuesta a incidentes	Desarrolle y mantenga un plan de respuesta ante incidentes.	Establecer un plan detallado para identificar, contener y mitigar las violaciones de datos, que incluya procedimientos de comunicación y coordinación con las autoridades reguladoras.
Encriptación de datos	Utilice técnicas de encriptación para proteger la PII tanto en tránsito como en reposo.	Encriptar los datos de los clientes utilizando algoritmos estándar del sector como los protocolos TLS/SSL.

Recursos en línea para obtener información adicional sobre la seguridad de la PII:

Nombre	Visión general de la información	Enlace URL
Asociación Nacional de Comisionados de Seguros (NAIC)	La NAIC ofrece recursos sobre la seguridad de datos, la normativa sobre privacidad y las mejores prácticas para los profesionales de los seguros.	https://www.naic.org/
Instituto de Información sobre Seguros (III)	El III ofrece información sobre ciberseguridad y protección de datos en el sector de los seguros, incluidos artículos y guías para agentes.	https://www.iii.org/
Comisión Federal de Comercio (FTC)	La FTC ofrece orientación sobre las leyes de seguridad y privacidad de los datos, incluidos recursos específicamente adaptados al sector de los seguros.	https://www.ftc.gov/
Centro de Recursos contra el Robo de Identidad (ITRC)	El ITRC ofrece información y recursos para ayudar a los agentes de seguros y a los consumidores a protegerse contra el robo de identidad y salvaguardar la información de los clientes.	https://www.idtheftcenter.org/