Security & Compliance

At InsuranceGPTs.com, we understand that security and compliance are paramount concerns for insurance professionals. Our commitment to maintaining the highest standards of data protection and regulatory alignment is reflected in every aspect of our platform design and operations.

Security Architecture

Zero-Data Storage Model

Our platform operates on a strict zero-data storage model:

- No client data is stored on our servers at any time
- All interactions are processed in real-time via OpenAI's secure infrastructure
- Data is not persisted after your session concludes
- No logging of sensitive information occurs within our systems

Transmission Security

While we don't store your data, we implement enterprise-grade security measures to protect data in transit:

- End-to-end encryption for all communications
- TLS 1.3 protocol implementation
- Strong cipher suites to protect data integrity
- Regular security certificate updates and monitoring

Infrastructure Security

Our platform infrastructure is built with security as a foundational principle:

- Regular vulnerability assessments and penetration testing
- Continuous monitoring for potential security threats
- Strict access controls for development and administrative team members
- Automatic security patch deployment

Compliance Framework

Regulatory Alignment

Our tools are designed with awareness of key insurance industry regulations, including:

- NAIC Model Laws and Regulations
- State-specific insurance regulations
- Privacy regulations including GLBA and applicable state privacy laws
- Relevant industry standards for insurance technology

PHI and PII Protection

We maintain strict controls to prevent the handling of protected information:

- Systems designed to avoid PHI/PII collection or processing
- No storage of personal health information as defined by HIPAA
- No retention of personally identifiable information
- No data mining or analysis of user inputs
- Technical safeguards to prevent inadvertent collection

Compliance by Design

Our development approach incorporates compliance considerations from inception:

- Regular compliance reviews of platform functionality
- Updates aligned with evolving regulatory requirements
- Documentation of compliance controls and safeguards
- Consultation with insurance compliance experts during design phases

Third-Party Security

OpenAI Integration

Our platform relies on OpenAI's infrastructure for processing, which includes:

- SOC 2 Type 2 certified infrastructure
- Enterprise-grade security controls
- Robust data protection measures
- Secure API endpoints with authentication requirements

Vendor Assessment

We conduct thorough security assessments of all technology vendors:

- Evaluation of security certifications and attestations
- Review of privacy practices and terms
- Monitoring of security track record and incident response

- Verification of compliance with relevant regulations

Independent Verification

Security Testing

Our platform undergoes regular independent security testing:

- Annual penetration testing by qualified third parties
- Vulnerability scanning on a continuous basis
- Code security reviews during development cycles
- Infrastructure configuration assessments

Compliance Reviews

We maintain a proactive compliance posture:

- Regular reviews by qualified compliance professionals
- Gap analysis against relevant regulatory requirements
- Documentation of compliance controls and their effectiveness
- Commitment to addressing compliance findings promptly

User Responsibilities

While we maintain robust security measures, effective security is a shared responsibility:

- Users should maintain secure access credentials
- Implement appropriate access controls within their organizations
- Follow professional guidelines for client information handling
- Ensure compliance with licensing requirements in their jurisdictions

Commitment to Improvement

Security and compliance are never "completed" but require ongoing commitment:

- Regular reassessment of security controls
- Monitoring of emerging threats and vulnerabilities
- Staying current with evolving regulatory requirements
- Continuous improvement of our security framework

Contact Information

For security or compliance inquiries:

- Email: support@insurancegpts.com

Last Updated: April 19, 2025