DigitalOwl

NAIC Model Bulletin Letter of Compliance

This Letter of Compliance addresses governance, risk management controls, and internal audit functions that DigitalOwl implements throughout its AI system life cycle in accordance with the NAIC Model Bulletin adopted in December 2023.

It should be noted that although DigitalOwl is not an insurance company and is not obligated to adhere to the NAIC Model Bulletin, it voluntarily chooses to align with its guidelines. This decision underscores DigitalOwl's dedication to providing customers with the highest level of service and assurance.

Governance

AI Governance Framework

DigitalOwl has developed an AI Governance toolkit that describes how transparency, fairness and accountability are maintained throughout the design and implementation of its AI system. DigitalOwl's AI Governance Toolkit is a comprehensive guide designed to help AI experts and governance committees evaluate DigitalOwl's AI solutions for use in the insurance industry, with a specific focus on their Natural Language Processing and Generative AI technologies for medical data analysis.

The toolkit covers key areas including AI principles and ethics, AI evaluation criteria (model description, data management, development and performance), contract terminology, regulatory compliance, and security measures. It emphasizes DigitalOwl's commitment to responsible AI deployment through robust data security, HIPAA and GDPR compliance, clear data ownership policies, and transparent decision-making processes, all while providing detailed evaluation checklists for thorough assessment of their AI system.

Proprietary and Trade Secret Information Protection

DigitalOwl is contractually obligated not to use any information provided by a third party for any purpose other than providing its services.

Governance (continued)

Policies and Procedures

DigitalOwl has created policies that encompass all aspects of privacy and security throughout the AI System lifecycle:

- Data Security Policy
- Information Security Roles and Responsibilities
- GDPR Data Breach and Response Plan
- Disaster Recovery Plan
- Data Retention Policy (GDPR)
- Data Protection by Design and Default Policy (GDPR)
- Data Management Policy and Procedures
- Data Classification Policy
- Data Backup and Restoration Policy
- Change Management Policy
- Business Continuity Plan
- Acceptable Use Policy
- Vulnerability Management Policy
- Technical and Organizational Measures (GDPR TOM)
- Risk Management Policy
- Privacy Impact Assessment Program
- Intrusion Detection (IDS) Policy
- Forensic Evidence Program
- External Suppliers Procedure
- Encryption Policy
- Asset Management Policy
- Security Incidents Procedure
- Logical Access Policy and Procedures
- Kubernetes Definition Guidelines

Compliance with Policies

DigitalOwl has developed a Compliance Program that includes the following:

- Experienced security and compliance team
- Awareness program for all employees including annual training and acceptance of Standards of Conduct and Acceptable Use Policy
- Internal audits on compliance with information security and privacy regulations
- External audits on information security controls and implementation
- Vulnerability audits in accordance with the Vulnerability Management Policy
- Annual risk assessment
- Annual policies review

Interdisciplinary Governance

DigitalOwl ensures comprehensive cross-departmental collaboration in the development, maintenance, and governance of AI systems.

- Collaboration of all departments including management in every aspect of the AI system development, maintenance, governance and oversight.
- Predefined roles and responsibilities related to every aspect of the AI system life cycle
- Monitoring, auditing, escalation, and reporting protocols and requirements.
- Employee Disciplinary Policy, Acceptable Use Policy, Standards of Conducts and Whistleblower Policy
- Annual training for all employees and end points monitoring

Risk Management and Internal Controls

Risk Management

DigitalOwl conducts an annual risk assessment that takes into account risks from different areas including AI, in accordance with its Risk Management Policy.

System Development Oversight

DigitalOwl ensures rigorous oversight across all phases of system development.

- Owasp's guidelines (including OWASP Top 10) are implemented by developers where applicable to maintain Software Development Life Cycle (SDLC)
- Segregation of development, testing, and operational environments
- Continuous monitoring of systems and services
- Vulnerability scans are conducted quarterly and prior to major version releases
- Strict due diligence on third party systems prior to engagement and annually thereafter
- Change Management policy that covers all of DigitalOwl's product and engineering systems and platforms used to operate and maintain its products and services
- Annual risk assessment
- 24/7 logs monitoring solution
- SDLC policies
- Change Management Policy
- Kubernetes Definition Guidelines
- Vulnerability Management Policy
- AI Development Policy
- Risk Management Policy
- Data Security Policy
- Intrusion Detection Policy
- Encryption Policy
- Logical Access Policy and Procedures
- Infosec Roles and Responsibilities
- Data Classification Policy
- Data Backup and Restoration Policy

Data Practices and Accountability

DigitalOwl uses robust processes for managing all aspects of data, from collection through use, while ensuring fairness and appropriateness.

- Data extraction is based on source documents and linked directly to them
- Full visibility into decision trees, query answers, and the logical flow leading to suggested decisions
- Regular audits of AI outputs to detect potential biases
- Diverse training data to ensure representation across different demographics
- Ongoing monitoring and adjustment of AI models to address any identified biases

Risk Management and Internal Controls (continued)

Validation and Testing

DigitalOwl implements a multi-layered validation and testing approach that includes the following:

- **Initial Validation:**
  - Uses statistical regression tests and manual quality assurance of sample cases for new models and successive model versions
  - Performs testing under conditions that mirror real-world scenarios
  - Validates against known medical records with expert-verified outcomes
- **Training/Test Split:**
  - Separates data for model development and validation
  - Uses unseen test data to evaluate model performance
- **Continuous Monitoring:**
  - Conducts daily sampling of cases to detect anomalies and data drift
  - Performs regular evaluation of processing outcomes against ground truth
  - Monitors operating conditions for system performance outside defined limits
  - Regular audits of AI outputs to detect potential biases
  - Diverse training data to ensure representation across different demographics
  - Ongoing monitoring and adjustment of AI models to address any identified biases
- **Expert Verification:**
  - Implements automatic quality checks on platform's final outputs
  - Uses outcome-driven tests comparing workflow decisions against expert assessments for sample cases
- **Performance Validation:**
  - Ongoing refinement of AI models based on performance metrics and user feedback
  - Quarterly internal audits of AI performance and decision quality

Protection of Non Public Information

DigitalOwl uses robust processes for managing all aspects of data, from collection through use, while ensuring fairness and appropriateness.

- Access control based on RBAC and least privilege principle
- Security tools such as IDS, DLP
- GDPR compliance
- HIPAA Compliance
- Annual training to all employees and acknowledgement of Acceptable Use Policy
- Data Protection related policies
- Privacy Policy
- Data Management Policy and Procedure
- Data Security Policy
- Data Retention
- Data Backup and Restoration

Risk Management and Internal Controls (continued)

External Third Party Management

External third parties are reviewed and evaluated in accordance with our External Suppliers Procedure

- Evaluating and considering the data security of external suppliers
- Signing applicable data related agreements (i.e. DPA, NDA, BAA)
- Documenting the due diligence process
- Review and approval by management

Access our AI Governance toolkit for a comprehensive overview of our AI principles and practices.