Institutional Review Board (IRB) Compliance & Data Security Overview

1. Data Confidentiality & Privacy Protection Intellectus prioritizes data confidentiality and employs industry-standard security measures to protect sensitive and personally identifiable information (PII). Data encryption is applied both in transit (using TLS 1.2+) and at rest to safeguard against unauthorized access. Role-based access controls ensure that only authorized personnel can access user data.

2. Compliance with Regulatory Standards While Intellectus is not specifically designed for storing Protected Health Information (PHI), we align with best practices for de-identification as outlined in the HIPAA Privacy Rule. Researchers are advised to de-identify PHI before uploading data.

3. Data Retention & Deletion Policy Intellectus retains user data only as long as necessary to provide services. Users may request deletion of their data at any time by contacting support. Automatic data purging occurs based on established retention policies, ensuring that outdated or unnecessary data is securely removed.

4. Third-Party Data Sharing & Cloud Storage Intellectus engages third-party service providers for infrastructure, IT services, and analytics. All third-party providers are vetted to meet industry security standards. User data is never used to train third-party AI models. Additionally, all data is stored in secure, geographically distributed data centers with strict access controls.

5. Data Breach & Incident Response Plan In the event of a data breach, Intellectus follows a structured incident response plan, including:

- Immediate assessment and containment of the breach.
- Notification of affected users within legally required timeframes.
- Coordination with relevant regulatory bodies and cybersecurity experts to mitigate risks.
- Implementation of corrective actions to prevent future incidents.

6. User Consent & Data Ownership Users maintain full ownership of their uploaded data. Intellectus does not claim rights over user research data and does not use user-generated content for purposes beyond service delivery. Researchers are encouraged to obtain informed consent from study participants before storing data on the platform.

7. Anonymization & De-Identification To enhance security, Intellectus recommends de-identification of sensitive datasets before uploading. Users should remove direct identifiers (e.g., names, social security numbers) and apply anonymization techniques where applicable. Researchers can leverage guidance from regulatory bodies to ensure compliance with data protection standards.

8. Use of Large Language Models (LLMs) Intellectus integrates LLMs for enhanced user experience, including natural language processing and analytical support. User

data processed by LLMs is not stored or used for model training. All interactions are subject to strict security protocols to prevent exposure of sensitive information.

9. Researcher Responsibilities & Best Practices

- Ensure proper de-identification of sensitive data before upload.
- Adhere to IRB and institutional data security policies.
- Regularly review and manage stored data to minimize security risks.
- Utilize strong authentication and access controls for research team members.

For additional questions regarding IRB compliance and data security, please contact: **info@intellectus360.com**