

## Data Protection Policy

CASK Research Foundation is committed to upholding the highest standards of data protection and safeguarding in all aspects of its operations, particularly concerning sensitive medical data. This policy outlines the principles and procedures to ensure the secure handling, processing, and sharing of sensitive medical information in compliance with applicable laws and regulations, including the General Data Protection Regulation (GDPR).

This policy applies to all employees, volunteers, contractors, and third parties involved in the collection, processing, and sharing of sensitive medical data on behalf of CASK Research Foundation.

The current Data Protection Officer is: Laura Hattersley

### 1. Overarching principles

**1.1. Confidentiality:** All sensitive medical data obtained by CASK Research Foundation shall be treated with the utmost confidentiality and respect for privacy.

**1.2. Anonymisation:** Families will always be asked to anonymise any medical data prior to sharing it with CASK Research Foundation. In addition, whenever possible, sensitive medical data collected from families shall be anonymised to prevent the identification of individuals. Anonymisation methods shall be employed prior to any data processing or sharing activities unless otherwise requested by the family.

**1.3. Informed Consent:** The charity shall obtain informed consent from individuals or their legal guardians before sharing any sensitive medical data with third parties. Consent forms shall clearly outline the purpose of data sharing and the identities of the recipients.

**1.4. Data Minimisation:** Only necessary and relevant sensitive medical data shall be collected, processed, and shared for the purpose of research conducted by CASK Research Foundation. Unnecessary data shall not be retained.

**1.5. Security Measures:** Appropriate technical and organisational measures shall be implemented to safeguard sensitive medical data against unauthorised access, disclosure, alteration, or destruction. This includes encryption, access controls, and secure storage systems.

**1.6. No Storage of Personal Medical Data:** CASK Research Foundation shall not store any personal medical data on its hard drives or internal systems. Data shall be securely stored on encrypted servers or cloud-based platforms with robust security measures in place.

### 2. Procedures

**2.1. Anonymisation Process:** Prior to the collection or sharing of sensitive medical data, the charity shall ensure that data is anonymised to the greatest extent possible. Anonymisation methods may include removing personally identifiable information or coding data to obscure identities.

**2.2. Informed Consent:** When obtaining consent for the collection or sharing of sensitive medical data, the charity shall provide clear and comprehensive information regarding the purpose, scope, and recipients of the data. Consent can be in the form of an email or a consent form shall signed by individuals or their legal guardians.

**2.3. Third-Party Sharing:** Before sharing sensitive medical data with third parties, the charity shall obtain explicit consent from individuals or their legal guardians. The charity shall also assess the data protection policies and practices of third parties to ensure adequate safeguards are in place.

**2.4. Data Handling Training:** All employees, volunteers, and contractors involved in the handling of sensitive medical data shall receive training on data protection principles, procedures, and legal requirements. Training shall be provided regularly to ensure ongoing compliance.

### **3. Compliance with GDPR**

3.1. CASK Research Foundation acknowledges and commits to abiding by the provisions of the General Data Protection Regulation (GDPR) regarding the processing and protection of personal data, including sensitive medical data.

3.2. The charity shall ensure that all processing of personal data, including sensitive medical data, is lawful, fair, and transparent, and conducted for specified, explicit, and legitimate purposes.

3.3. Individuals shall have the right to access their personal data held by CASK Research Foundation, as well as the right to rectification, erasure, and restriction of processing in accordance with GDPR requirements.

3.4. The charity shall implement appropriate technical and organisational measures to ensure the security of personal data, including sensitive medical data, and mitigate the risk of data breaches.

### **4. Liability**

4.1. CASK Research Foundation shall not be held liable for any breaches of confidentiality or data protection resulting from the unauthorised disclosure or sharing of sensitive medical data by individuals or families.

### **5. Compliance and Review**

5.1. Compliance with this policy is mandatory for all individuals and entities associated with CASK Research Foundation. Any violations of this policy shall be subject to disciplinary action, up to and including termination of employment or contract.

5.2. This policy shall be reviewed regularly to ensure ongoing compliance with applicable laws, regulations, and best practices in data protection and safeguarding.

### **6. Conclusion**

CASK Research Foundation is committed to ensuring the privacy, confidentiality, and security of sensitive medical data entrusted to its care. By adhering to the principles and procedures outlined in

this policy, the charity aims to uphold the trust and confidence of individuals and families participating in its research initiatives.