**Institution 1: MedTech University Research Center (MURC)**

**1. Data Privacy:**

MedTech University Research Center (MURC) enforces stringent data privacy policies, particularly regarding the handling of personal data in medical research. All data collected must undergo anonymization prior to analysis. The anonymization process entails removing direct identifiers (e.g., names, social security numbers, and addresses) and replacing them with unique codes. Furthermore, researchers must ensure that no re-identification of subjects can occur without proper legal or ethical justification.

* **Informed Consent**: All participants must provide informed consent, specifically stating how their data will be used, stored, and anonymized. This consent must clearly indicate that participants can withdraw at any point without consequences, and their data will be excluded from future analysis.
* **Access Controls**: Only authorized personnel are allowed to access raw personal data before anonymization. MURC limits access to a maximum of 10 researchers, each of whom must undergo annual training on data security and privacy best practices. A role-based access control system is in place to ensure that data can only be accessed by researchers who need it for their role.
* **Audit Trail**: All access to personal data must be logged. MURC retains logs for at least 5 years, ensuring traceability and accountability for any data access.
* **Data Breach Response**: In case of a data breach, MURC has implemented a rapid response plan. Any breach involving personal or sensitive data must be reported within 24 hours to the relevant authorities, including internal data protection officers and external regulatory bodies. Mitigation actions must be initiated within 12 hours of detection to prevent further breaches.

**2. Data Storage:**

MURC mandates that all research data be stored in encrypted databases, with encryption protocols adhering to industry standards (AES-256 encryption for data at rest and TLS for data in transit). Personal data must be stored separately from anonymized datasets to minimize the risk of identification in case of a breach.

* **Data Retention**: Personal data must be retained for 5 years following the completion of a study, after which it must be deleted unless there is a legal requirement to keep it for longer. Anonymized data can be retained for up to 10 years for future research purposes, provided that no re-identification process is possible.
* **Backup and Recovery**: MURC performs automated weekly backups of all research data, ensuring that backups are encrypted and stored in a separate secure facility. In case of data corruption or loss, the backup system allows for full data recovery within 48 hours.
* **Disposal**: Upon completion of the 10-year retention period for anonymized data, MURC enforces secure data disposal protocols, including the use of certified data erasure software and physical destruction of storage devices.

**3. Compliance with GDPR**:

Given its location within the European Union, MURC complies with the General Data Protection Regulation (GDPR). As such, it appoints a Data Protection Officer (DPO) responsible for overseeing data handling practices, responding to data subject requests, and ensuring the institution remains compliant with evolving regulatory requirements.