How We Protect Your Research Data

Thank you for taking part in research. Your participation makes scientific progress possible, and we are committed to protecting your information and maintaining the trust you have placed in us. When this study ends, the data we collect from you are sent to the NIDDK Central Repository (NIDDK-CR), an NIH Controlled-Access Repository. Recently, someone misused data from a major brain development study. Although this incident did not involve NIDDK-CR, it reminds everyone in the research community of the importance of protecting research data. The NIDDK-CR wants to explain the security measures they use to keep research data safe.

Who can access the data? Only qualified researchers are allowed to apply to use data in the NIDDK-CR repository. Before researchers are approved, NIDDK-CR repository staff confirm researchers identity through their university or research institution. An official at their institution must also confirm that the researcher is a permanent employee and meets eligibility requirements. The repository performs additional security checks to make sure people are who they claim to be. Each researcher must sign a legally binding agreement that says they will use the data only for an approved research project. Their institution must also provide official confirmation that they have security requirements in place for handling sensitive information. The NIDDK-CR also works with other NIH data repositories to block known bad actors from gaining access. Researchers cannot access the data anonymously or without oversight from their institution.

How does NIDDK-CR monitor data use? NIDDK-CR does not just grant access and forget about it. They actively monitor how researchers use the data after access is granted through mandatory annual reviews. Every year, researchers must submit a yearly report describing their progress and confirm that they are following the rules. They may use the data only for the specific project that was approved. If a researcher does not follow the agreement, misses required reports, or uses the data in ways that were not approved, NIDDK-CR can suspend or permanently remove their access. NIDDK-CR also notifies the researcher's institution if this happens and may suspend access to everyone at that institution. When a project ends, researchers must provide written proof that they have destroyed all copies of the data. The repository also reviews published research studies to make sure the data were used properly as approved and investigates any concerns.

Strengthening data security. NIDDK-CR recognizes that determined bad actors can sometimes deceive even strong security systems, so they are working to strengthen security by developing a secure online research environment. This system operates behind a federal firewall and allows researchers to analyze data without downloading it to their own computers. Because the data stay within NIDDK-CR's protected system, the risk of improper sharing is greatly reduced. This approach adds another layer of protection to data that are already safeguarded under strict security standards. Protecting the data you have contributed to research is a responsibility NIH and NIDDK-CR take very seriously. They regularly review and improve their security practices to maintain high standards of data protection. Your trust is essential to advancing research, and safeguarding your information remains central to their mission.