Homework 6: Reflecton.

Reflect on your previous work and how you would adjust to include ethics and inequity components. Total length should be a few paragraphs, no more than one page.

To ensure adherence to ethical standards in our data work at my previous job, we implemented several rules:

1. **Randomization of Training and Testing Databases**: All training and testing databases contained randomly mixed personal information. Personal information could be randomly scrambled to prevent identification.
2. **Limited Access to Real Data in Debugging**: If bugs were related to data in the database, developers could request real data for debugging purposes. However, only a few rows of data were provided, not the entire database.
3. **Use of Unpopular Hierarchical Database Management Systems (DBMS)**: Our databases were developed using unpopular hierarchical DBMS, which would pose challenges for unauthorized access and data leakage.
4. **Decentralized Database Access**: Our databases were spread out and did not have a single access point, enhancing security by limiting access to specific datasets.
5. **Verification of Internal Storage Before Input**: All internal storages were checked before being inputted into the workstations, ensuring data integrity and security.

These steps were crucial for maintaining security and preventing inappropriate access and personal information leakage. However, in cases where modeling on testing databases proved impossible or yielded insufficient results, developers could request access to the full database, potentially increasing the risk of breaching ethics rules.

To further enhance safety measures, I suggest implementing log and tracking tools to monitor data access and usage.

On one occasion, our personnel encountered a cybersecurity threat in the form of email spam with viruses. Some computers within our network were infected; fortunately, no data was compromised because the infected computers lacked access to the data. Despite this, I recommend adding "cyber hygiene" to the ethics guidelines for all staff members connected to networks with database storage to bolster our defenses against such threats.