Report in Brief

Date: February 2019
Report No. A-18-18-09350

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Why OIG Did This Review

As part of the Department of Health and Human Services (HHS), the National Institutes of Health (NIH) is the largest public funder of biomedical research agency in the world, investing more than $30 billion in taxpayer dollars to achieve its mission. NIH's mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability. OIG has identified risks related to the sharing of sensitive data.

Our objective was to assess whether NIH had adequate controls in place when permitting and monitoring foreign principal investigators' (PIs) access to NIH genomic data.

How OIG Did This Review

We reviewed NIH's internal controls for monitoring and permitting access to foreign PIs. To accomplish our objective, we used appropriate procedures from applicable Federal regulations and guidance. We reviewed NIH policies, procedures, and supporting documentation, and we interviewed NIH staff.

Opportunities Exist for the National Institutes of Health To Strengthen Controls in Place To Permit and Monitor Access to Its Sensitive Data

What OIG Found

NIH did not consider the risk presented by foreign PIs when permitting access to United States genomic data. NIH expects foreign PIs to safeguard NIH data and use sound security practices in accordance with signed user agreements entered into with the respective NIH Institute or Center. However, NIH has not assessed the risks to national security when permitting data access to foreign PIs. We also found that NIH does not verify that foreign PIs have completed security training, even though NIH's Security Best Practices for Controlled-Access Data emphasize security training as a key control.

What OIG Recommends and NIH Comments

We recommend that NIH work with an organization with national security expertise and knowledge of international risk areas to assess the impact of the potential misuse of genomic data provided to foreign PIs. NIH could strengthen its controls by developing a security framework, conducting a risk assessment, and implementing additional appropriate security controls designed specifically for foreign PIs that have access to genomic data that includes United States citizens. We also recommend that NIH develop and implement mechanisms to ensure that the Genomic Data Sharing Policy keeps current with emerging threats to national security. Lastly, we recommend that NIH make security training and security plans a requirement and develop additional internal controls to verify that foreign PIs and entities have fulfilled those requirements.

NIH did not concur with our recommendations to develop a security framework, conduct a risk assessment, and implement additional controls for sensitive data. NIH concurred with our recommendations to ensure security policies keep current with emerging threats and to make training and security plans a requirement; however, NIH did not agree to the addition of controls to ensure training and security plan requirements have been fulfilled.

We maintain that our findings and recommendations are valid. We recognize that NIH reported that it is already taking certain actions, that may address recommendations. We provided NIH with other potential actions to address our findings.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181809350.asp.