Report in Brief
Date: June 2019
Report No. A-18-17-09304

U.S. Department of Health & Human Services
Office of Inspector General

The National Institutes of Health Could Improve Its Monitoring To Ensure That an Awardee of the *All of Us* Research Program Had Adequate Cybersecurity Controls To Protect Participants' Sensitive Data

Why OIG Did This Review

The *All of Us* Research Program (*All of Us*) is a major component of the Precision Medicine Initiative. *All of Us* is responsible for building a national research cohort of more than 1 million participants who will provide their personal health information to the National Institutes of Health (NIH) so researchers, providers, and patients can work together. Ensuring that participant data are securely maintained is paramount to retaining the participants' trust and participation in *All of Us*.

Our objective was to determine whether NIH ensured that two awardees that provide support for *All of Us* had adequate controls to protect participants' sensitive data.

How OIG Did This Review

We reviewed information system general controls at two of the seven components of the *All of Us* program: the Participant Technology Systems Center (PTSC), awarded to Vibrent Health, and the Data and Research Center, awarded to Vanderbilt University Medical Center. These controls included security plans, access controls, information protection and system maintenance, audit logging, data and physical security, incident response, and disaster recovery. To accomplish our objective, we used appropriate procedures from applicable Federal requirements and guidance.

What OIG Found

The PTSC did not have adequate controls to protect *All of Us* participants' sensitive data. NIH did not adequately monitor the PTSC to ensure that the PTSC had implemented adequate cybersecurity controls to protect the participants' sensitive data. Based on the results of our penetration testing at the PTSC, we identified vulnerabilities that could expose personally identifiable information, including personal health information of the *All of Us* participants, and allow access to their data. These vulnerabilities could have allowed an attacker with limited technical knowledge to exploit and compromise the PTSC's systems, as most of the vulnerabilities did not require significant technical knowledge to exploit. In addition, the PTSC failed to enable encryption in the S3 buckets used for cloud storage. The PTSC did not have policies and procedures to address remediating source code vulnerabilities and timely disabling of network access. Finally, the PTSC did not adequately scan its network.

During the audit, NIH and the PTSC addressed and remediated all of the vulnerabilities we identified.

We did not identify any general control vulnerabilities at the Data and Research Center.

What OIG Recommends and NIH Comments

We recommend that NIH revise its *All of Us* Cooperative Agreements and cooperative agreements with security and privacy requirements to include a detailed description of how NIH will monitor cybersecurity and ensure that future awardees adequately implement security controls to protect sensitive data.

In written comments on our draft report, NIH requested that we revise our recommendation to limit the scope of applicability to "appropriately focus on those cooperative agreement awards with security and privacy requirements," which we have done. NIH stated that, based on our recommendation, it is reviewing *All of Us* Research Program awards. Specifically, NIH stated that it will make necessary updates to security and privacy terms and conditions.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/181709304.asp.