Department of Health and Human Services
Office of Inspector General
Office of Audit Services

September 2025 | A-18-24-06111

The National Institutes of Health Needs to Improve the Cybersecurity of the *All of Us* Research Program to Protect Participant Data

REPORT HIGHLIGHTS

September 2025 | A-18-24-06111

The National Institutes of Health Needs to Improve the Cybersecurity of the *All of Us* Research Program to Protect Participant Data

Why OIG Did This Audit

- The goal of NIH's *All of Us* Research Program is to advance disease prevention and treatment by making personal health information provided by more than 1 million volunteer participants available for research.
- The Data and Research Center (DRC) houses the participant data and is managed by an NIH award recipient. This audit examined whether NIH ensured that the DRC award recipient: (1) adequately limited access to research data, (2) implemented required information security and privacy controls, and (3) remediated information security and privacy weaknesses in accordance with Federal requirements.
- It is crucial for NIH to protect research participants' personal health data from cybersecurity and national security threats.

What OIG Found

The DRC award recipient implemented some cybersecurity controls to protect participant data; however, NIH did not:

- ensure that the DRC award recipient limited the access of authorized data users to program data in accordance with program policies,
- communicate national security concerns associated with maintaining genomic data to the DRC award recipient to enable it to choose the appropriate security and privacy cybersecurity controls for its information systems, and
- ensure that security and privacy weaknesses were remediated within federally required timeframes.

What OIG Recommends

We made five recommendations to NIH to improve its oversight of the *All of Us* Research Program's DRC, including that NIH require the DRC award recipient to implement access controls to limit access to information systems and detailed participant data, and to reevaluate its security categorizations. The full recommendations are in the report.

NIH concurred with all five of our recommendations.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

Persistent cybersecurity and national security threats exacerbate the challenges associated with protecting the data and technologies used to carry out National Institutes of Health (NIH) programs. Cyberattacks can imperil critical operations and programs, and potentially compromise sensitive data. It is crucial for NIH to protect personal health data, including from participants in NIH's *All of Us Research Program* (*All of Us*), from cybersecurity and national security threats.

OBJECTIVES

Our objectives were to determine whether NIH ensured that the *All of Us* award recipient for the Data and Research Center (DRC): (1) limited access to program research data, (2) implemented required information security and privacy controls, and (3) remediated information security and privacy weaknesses in accordance with Federal requirements.

BACKGROUND

Precision Medicine Initiative

In 2015, the Precision Medicine Initiative (PMI) was announced to revolutionize how we improve health and treat disease. The goal of the PMI is to transform disease prevention and medical treatment such that they can be tailored by considering individual variability in genes, environment, and lifestyle. Precision medicine gives clinicians tools to better understand the complex mechanisms underlying a patient's health, disease, or condition, and to better predict which treatment will be most effective. One of the key parts of the PMI was for NIH to develop a voluntary national research cohort of 1 million or more volunteers to propel their understanding of health and disease and set the foundation for a new way of doing research through engaged participants and open, responsible data sharing. NIH launched its PMI cohort program—*All of Us*—in October 2016.

Privacy and Security of Data in the Precision Medicine Initiative

In March 2015, the White House convened an interagency working group to develop *Privacy and Trust Principles* (Principles) for the PMI.[1] The resulting Principles are governance; transparency; participant empowerment; respect for participant preferences; data sharing, access, and use; and data quality and integrity. These Principles provide broad guidance for PMI activities. The interagency working group also took steps to build security practices into the PMI to ensure the confidentiality and integrity of all PMI data and created the *Data Security*

[1] The interagency working group was co-led by the White House Office of Science and Technology Policy, the Department of Health and Human Services' Office for Civil Rights, and NIH.

Policy Principles and Framework (Security Framework). The Security Framework recognizes that there is no "one size fits all" approach to managing data security and provides a broad framework for protecting participants' data. It also states that PMI organizations will comply with all applicable laws and regulations governing privacy, security, and the protection of PMI data at every stage of data collection, storage, analysis, maintenance, use exchange, and dissemination.

All of Us Research Program

The aim of *All of Us* is to advance disease prevention and treatment by using personal health information from more than 1 million participants. The participant data consist of more than 470,000 electronic health records and 607,000 biosamples.[2, 3] NIH designed *All of Us* to enable research on a wide range of diseases—both common and rare—and detect associations between genetic and environmental exposure and a wide variety of health outcomes.[4] Through traditional research funding instruments (e.g., grants, contracts) as well as agreements made under its other transaction authority, [5] NIH established nine *All of Us* program units: (1) Biobank, (2) Communications and Engagement Partners, (3) DRC, (4) Health Care Provider Organizations, (5) Participant Center, (6) Participant and Partner Services Center, (7) Genomics Partners, (8) Center for Linkage and Acquisition of Data, and (9) Partnered Research Studies.

Data and Research Center

In 2016, NIH awarded an agreement for the creation and management of the DRC. The DRC develops and maintains the DRC information system that contains the database of information provided by *All of Us* participants and focuses on ensuring the data are organized and secure. The DRC also manages researchers' access to and use of sensitive participant data through the DRC Researcher Workbench (DRC-RW), which is a subsystem of the DRC information system. The DRC-RW is a cloud-based information system that provides registered researchers with tools to support data analysis and collaboration, such as workspaces to access, store, and analyze data for specific research projects and analysis tools to perform queries within *All of Us* datasets.

---

[2] As of May 28, 2025, over 1.4 million individuals had registered for All of Us, and of those, more than 746,000 completed initial program steps to contribute their data. There are four levels of participation: interested, registered, consented, and participant. For more information, see All of Us, "Data Snapshots." Accessed May 29, 2025.

[3] The biosamples collected include participants' blood, urine, and saliva samples.

[4] "*All of Us* Research Program, Operational Protocol," pg. 13.

[5] An "other transaction" is a unique type of legal instrument other than a contract, grant, or cooperative agreement. Generally, this awarding instrument is not subject to the Federal Acquisition Regulation or grant regulations unless otherwise noted in the terms and conditions of award.

The DRC and DRC-RW information systems contain data that are classified into three tiers:

- The Public Tier contains only aggregate data with identifiers removed and is available to everyone. Individuals do not need to register for Public Tier access and may access a publicly available data browser and data snapshots.

- The Registered Tier contains data from electronic health records (EHRs), wearable devices, and surveys, and can only be accessed by registered researchers.[6, 7]

- The Controlled Tier contains the same data as the Registered Tier as well as genomic data and demographic data from EHRs and surveys, and can only be accessed by registered researchers.[8]

HHS Office of National Security

Within the Department of Health and Human Services' (HHS's) Immediate Office of the Secretary, the Office of National Security (ONS) manages departmentwide programs and provides oversight, policy direction, standards, and performance assessments in the areas of intelligence, counterintelligence, insider threat, cyber threat intelligence, information security, national personnel security, homeland security, and the safeguarding of classified information. ONS provides NIH, along with other HHS operating divisions, with information related to foreign adversarial intents to access sensitive U.S. technologies and data, including genomic data, on a regular basis. ONS deemed the protection of *All of Us* participants' personally identifiable information (PII), including genomic data, to be a national security concern.

HOW WE CONDUCTED THIS REVIEW

We reviewed NIH's policies and procedures and the DRC awardee's policies and procedures for managing the DRC and DRC-RW information systems that were in place during our March 2024 site visit. We also reviewed the current agreement to manage the DRC, which was signed by NIH and the DRC awardee in November 2023. In addition, we reviewed and tested select information system security and privacy controls for the DRC and DRC-RW information systems including system security plans (SSPs), contingency planning and disaster recovery, security awareness and training, risk assessment, vulnerability scanning, incident response, flaw

[6] All of Us has a formal registration process for researchers that includes identity verification and training. For more information, see "All of Us Registration." Accessed June 4, 2025.

[7] For this audit, we refer to any person who is authorized to access and/or work with Registered or Controlled Tier data from the All of Research Program as an "authorized data user," which is the terminology used in the All of Us *Data User Code of Conduct*. For more information, see "*Data User Code of Conduct*." Accessed June 4, 2025.

[8] For this audit, we grouped Registered and Controlled Tier data together and refer to them as "detailed participant data" since both tiers contain sensitive personal information of All of Us participants.

remediation, plan of action and milestones, penetration testing, access controls, physical and environmental protection, and system monitoring.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology. Appendix B contains specific Federal requirements and guidance.

FINDINGS

We found that the DRC awardee implemented security controls for contingency planning and disaster recovery, security awareness and training, vulnerability scanning, incident response, flaw remediation, plan of action and milestones, penetration testing, physical and environmental protection, and system monitoring. However, NIH did not ensure that the DRC awardee (1) implemented controls to limit access to program research data in accordance with program policies, (2) implemented required information security and privacy controls for the DRC and DRC-RW information systems, and (3) remediated information security and privacy weaknesses in accordance with Federal requirements.

The DRC awardee's policies and procedures for the DRC and DRC-RW information systems allow authorized data users to remotely access the systems from foreign countries with prior approval, but the DRC awardee did not implement access controls to restrict remote access solely to individuals who had received approval. The *All of Us Data Use Policies* prohibit authorized data users from downloading detailed participant data, but the DRC-RW information system did not have access controls in place to prevent them from downloading the data. Also, NIH had not informed the DRC awardee about the national security concerns and increased risks associated with maintaining genomic data, and these factors should have been considered when selecting the set of information system security and privacy controls to implement. Further, the DRC awardee did not remediate weaknesses identified within the timeframe requirements stated in its award agreement with NIH. As a result of these findings, there was an increased risk of a bad actor gaining unauthorized access to the DRC or DRC-RW information systems due to inadequate access controls, and they could download and misuse the genomic data of *All of Us* participants.

THE DRC AWARDEE DID NOT IMPLEMENT ACCESS CONTROLS TO PREVENT AUTHORIZED INTERNAL USERS FROM ACCESSING DATA WHILE ABROAD WITHOUT PRIOR APPROVAL

According to the *DRC User Policies and Procedures*, staff who want to access the DRC information system while abroad must complete a *Working from Abroad with PMI Accounts* survey in advance. The survey, which contains user account and travel information, is sent to

the DRC's security staff. When a user accesses the DRC information system while abroad, the security staff uses information from the survey to verify that the user is authorized to access the system while abroad and can monitor the account for any potentially malicious or unusual activity.

We determined that the DRC awardee did not implement access controls to prevent authorized internal users from accessing the DRC and DRC-RW information systems while abroad without prior approval. We determined that the DRC awardee did not implement access controls to prevent internal users who did not complete a *Working from Abroad with PMI Accounts* survey in advance from accessing the DRC and DRC-RW information systems while abroad. Specifically, our testing of the systems' access controls determined that, when staff accessed the DRC and DRC-RW information systems while abroad, a system-generated warning appeared via a pop-up notification stating that their access would be restricted if documentation of their approval to use the systems while abroad was not provided within 24 hours. However, the controls did not prevent them from continuing to access and use the systems during that initial log in.

The lack of a system control to prevent internal users from accessing the DRC or DRC-RW information systems while abroad without prior approval does not allow the DRC to identify and assess the risks associated with this activity in the location and possibly take measures to ensure the protection of the data.

THE DRC AWARDEE DID NOT IMPLEMENT ACCESS CONTROLS TO PREVENT THE DOWNLOADING OF DETAILED PARTICIPANT DATA

The *All of Us Data Use Policies* state that authorized data users are prohibited from downloading detailed participant data. Our testing determined that the DRC-RW information system access controls did not prevent authorized data users from downloading detailed participant data.[9] When an authorized data user attempted to download detailed participant data from the DRC-RW information system—regardless of their location—a warning banner appeared with a message indicating that the user was prohibited from downloading the data. However, the authorized data user could download the detailed participant data, which is prohibited by policy, by checking a box just below the warning message that stated: "I understand the data use policies and certify that this download will be used in accordance with *All of Us* Data Use Policies."

The DRC awardee confirmed that there were no access controls in place to prevent the downloading of detailed participant data. The DRC awardee stated that the DRC-RW information system cannot distinguish the type of data an authorized data user is downloading; therefore, it cannot create a system control to prevent it.

[9] Our testing only indicated the possibility of downloading detailed participant data and did not include testing to determine if detailed participant data had actually been downloaded.

Without a control to prevent the downloading of detailed participant data, the confidentiality of sensitive genomic and participant data is at increased risk if the downloaded detailed data is viewed by unauthorized people.

THE DRC AWARDEE DID NOT CONSIDER NATIONAL SECURITY CONCERNS OF MAINTAINING GENOMIC DATA IN DETERMINING THE MINIMUM SET OF INFORMATION SECURITY AND PRIVACY CONTROLS TO IMPLEMENT

The National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199 requires organizations to determine the security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS Publication 200 requires organizations to select a minimum set of security and privacy controls based on the security categorization of the information system.

The DRC awardee, in coordination with NIH, used FIPS guidance to determine that the security categorization for the DRC and DRC-RW information systems was moderate risk.[10] The DRC awardee, with NIH's agreement, chose to include additional controls beyond the minimum set for a moderate-risk system. However, ONS had deemed genomic data to have national security and economic implications and systems that maintain genomic data or information containing genomic data, or process such data, should be classified as high-risk. ONS informed HHS and its operating divisions, including NIH, about the national security implications associated with genomic data through briefings, working groups, and weekly reports. NIH officials stated that they were aware of the national security concerns shared by ONS regarding genomic data but that they had not informed the DRC awardee about the concerns. The DRC awardee confirmed that, prior to a site visit we conducted for our audit, it was unaware of the concerns and the ONS requirement to categorize genomic data and systems that process such data as high risk.

Because the DRC awardee did not categorize the data and DRC and DRC-RW information systems as high risk, all the information security and privacy controls required to protect high risk systems were not selected and implemented. As a result, the processing, storage, or transmission of genomic data in the DRC and DRC-RW information systems may have been at risk of exploitation by bad actors.

[10] FIPS Publication 199 requires organizations to categorize systems as low-impact, moderate-impact, or high-impact for the stated security objectives of confidentiality, integrity, and availability. The control baselines selected for systems are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, or the Nation if there is a loss of confidentiality, integrity, or availability.

THE DRC AWARDEE DID NOT REMEDIATE INFORMATION SECURITY AND PRIVACY WEAKNESSES IN ACCORDANCE WITH ITS AWARD AGREEMENT

According to the November 2023 renewal of the award agreement between NIH and the DRC awardee, information security and privacy weaknesses identified as critical should be remediated within 15 days in accordance with Federal requirements. The requirements also state that those identified as high should be remediated within 30 days, moderate weaknesses should be remediated within 90 days, and weaknesses identified as low should be remediated within 1 year.

The DRC awardee chose to test its systems more frequently than what is required and has communicated its test results to NIH through monthly continuous monitoring meetings and reports. Also, the DRC awardee documented all identified weaknesses in its plan of action and milestones, which it shared with NIH.[11] However, the DRC awardee did not remediate information security and privacy weaknesses in accordance with the timelines documented in its award agreement with NIH which are based on Federal requirements. The DRC awardee remediated weaknesses based on longer timeframes documented in its SSPs for the DRC and DRC-RW information systems. Specifically, in the February 2024 versions of the SSPs, the weakness remediation timeframes were 30 days for weaknesses identified as critical, 60 days for those identified as high, and 1 year for those identified as medium or low which do not meet the Federal requirements. Although the DRC awardee has remediated or obtained a waiver for remediating the weaknesses within the timeframes listed in its SSPs, longer remediation timeframes allow bad actors additional time to take advantage of the weaknesses.

RECOMMENDATIONS

We recommend that NIH:

- require the DRC awardee to implement access controls to prevent DRC and DRC-RW information systems users from accessing the systems while abroad without verified approval;

- require the DRC awardee to identify and implement a control or compensating control to prevent the downloading of detailed participant data, as required by the *All of Us Data Use Policies*;

- formally communicate national security concerns related to maintaining genomic data to *All of Us* award recipients that use or maintain genomic data and require the

[11] A plan of action and milestones identifies tasks that need to be accomplished to remediate a weakness or gap in controls. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

implementation of the IT security and privacy controls to protect the storage, transmission, and processing of such data;

- require the DRC awardee to reevaluate the security categorization for the DRC and DRC-RW information systems considering the national security concerns of maintaining genomic data; and

- require the DRC awardee to update the remediation timeframe in its system security plans to comply with the timeframes specified in its award agreement with NIH.

NIH COMMENTS

In written comments on our draft report, NIH concurred with all five of our recommendations and described actions it has taken and plans to take to address them.

Regarding our first recommendation, NIH stated that the DRC awardee has implemented processes to prevent any user from accessing systems from countries of concern as well as a robust process by which DRC-RW users and their institutions are vetted to receive credentials permitting access to systems from inside the United States or abroad, as long as they are not accessing the systems from countries of concern. NIH further stated that it implemented processes for its verified internal users with privileged credentials to notify their intent in advance to access systems from abroad and create alerts to identify when users with privileged credentials access sensitive areas of the DRC and DRC-RW from outside the United States.

Regarding our second recommendation, NIH stated that the *All of Us* research program has implemented compensating controls to minimize the impact of these actions while maintaining the ability for researchers with *All of Us* data to download the results of their analyses that are needed to publish or otherwise disseminate their findings. NIH stated that the DRC awardee and the *All of Us* program have explored alternatives and decided that the current posture is best suited to meet the *All of Us* research program's policies without creating undue barriers to research. NIH further stated that it will conduct a review of the current posture of controls and compensating controls.

Regarding our third recommendation, NIH stated that it has implemented a technical update to enhance security measures focused on protecting data provided by NIH Controlled-Access Data Repositories. Specifically, as of April 4, 2025, NIH began prohibiting access to the repositories and associated data by institutions located in countries of concern. NIH also stated that it updated and formally communicated its implementation access practices and plans to issue additional requirements in the future.

Regarding our fourth recommendation, NIH stated that the DRC awardee is slated to renew its authority to operate in 2026 and that security categorization will be a key component of NIH's evaluation.

Finally, regarding out fifth recommendation, NIH stated that the *All of Us* research program swiftly implemented OIG's recommendation with the DRC awardee to create a milestone within its plan of action and milestones. NIH also stated that it updated its system security plan language to align with the updated timeline in the award agreement.

NIH's comments are included in their entirety in Appendix C.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We reviewed and tested some of the information system general controls of the DRC and DRC-RW information systems that were in place during our March 2024 site visit. These general controls included security plans, contingency planning and disaster recovery, security awareness and training, risk assessment, vulnerability scanning, incident response, flaw remediation, plan of action and milestones, penetration testing, access controls, physical and environmental protection, and system monitoring. We also reviewed the current agreement to manage the DRC, which was signed by NIH and the DRC awardee in November 2023.

We performed audit work from November 2023 through June 2025.

METHODOLOGY

To accomplish our objective, we:

- reviewed applicable Federal requirements and guidance and NIH policies and procedures;
- reviewed NIH awardee documentation between the DRC awardee and NIH for the DRC;
- reviewed NIH policies and procedures related to information security and privacy controls;
- reviewed DRC policies and procedures;
- examined and tested selected information system security and authorization documentation to include security assessment reports, vulnerability reports, internal and independent third-party security reports, supporting remediation documentation, security authorization(s) to operate, and system security plans;
- interviewed appropriate program officials from NIH and the DRC awardee; and
- discussed our findings with NIH officials.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: FEDERAL REQUIREMENTS

THE WHITE HOUSE

The *Achieving the Principles through a Precision Medicine Initiative Data Security Policy Framework* (January 26, 2022) states:

> PMI organizations should develop a comprehensive risk-based security plan that outlines roles and responsibilities related to security, consistent with the principles and framework outlined here. The security plan should identify the governance body for the organization's security program. The governance body will ensure that those who use or manage PMI data adhere to the security plan.[12] The security plan should be reviewed by the governance body and updated periodically to incorporate evolving standards and best practices. The plan should describe its approach for:
>
> - complying with applicable laws and regulations, and other organization-specific security policies and standards;
> - designating and maintaining an appropriately resourced and technically experienced information security team;
> - identifying, assessing, and responding to vulnerabilities and threats;
> - conducting continuous monitoring;
> - responding to security incidents and breaches;
> - ensuring the physical security of areas where PMI data is located, as well as that appropriate administrative and technical controls are in place to safeguard the data; and
> - ensuring participants, researchers, vendors, contractors, and technical staff are aware of their security responsibilities.
>
> PMI organizations should have an independent review of their security plans and of the effectiveness of controls on a periodic basis. The reviewer, at a minimum, should perform: a review of the organization's adherence to its security plan; regular vulnerability assessments (e.g., network scans, penetration testing, and assessments to protect against social engineering attacks); and evaluation and adjustment of the security program in light of vulnerability assessments and evolving circumstances.

[12] See governance principles outlined in NIH's *Precision Medicine Initiative: Privacy and Trust Principles*.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

Publication 199: *Standards for Security Categorization of Federal Information and Information Systems*

Security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Publication 200: *Minimum Security Requirements for Federal Information and Information Systems*

These standards require that each organization:

1. determines the security category of its information system in accordance with FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*;
2. derives the information system impact level from the security category in accordance with FIPS 200; and
3. applies the appropriately tailored set of baseline security controls in NIST Special Publication (SP) 800-53, Revision 5*, Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST SP 800-53, REVISION 5, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

Access Control (AC), AC-1, Policy and Procedures

Control:

a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
b. access control policy that:
    1. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
c. Procedures to facilitate the implementation of the access control policy and the associated access controls;
d. Designate an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures; and

e. Review and update the current access control:
    1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
    2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

AC-3, Access Enforcement

Control: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

AC-6, Least Privilege

Control: Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Planning (PL), PL-2, System Security and Privacy Plans

Control:

a. Develop security and privacy plans for the system that:
    1. Are consistent with the organization's enterprise architecture;
    2. Explicitly define the constituent system components;
    3. Describe the operational context of the system in terms of mission and business processes;
    4. Identify the individuals that fulfill system roles and responsibilities;
    5. Identify the information types processed, stored, and transmitted by the system;
    6. Provide the security categorization of the system, including supporting rationale;
    7. Describe any specific threats to the system that are of concern to the organization;
    8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
    9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
    10. Provide an overview of the security and privacy requirements for the system;
    11. Identify any relevant control baselines or overlays, if applicable;
    12. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
    13. Include risk determinations for security and privacy architecture and design decisions;
    14. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and

15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];
c. Review the plans [Assignment: organization-defined frequency];
d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
e. Protect the plans from unauthorized disclosure and modification.

Risk Assessment (RA), RA-2, Security Categorization

Control:

a. Categorize the system and information it processes, stores, and transmits;
b. Document the security categorization results, including supporting rationale, in the security plan for the system; and
c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

RA-5, Vulnerability Monitoring and Scanning

Control:

a. Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyze vulnerability scan reports and results from vulnerability monitoring;
d. Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
e. Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and
f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

APPENDIX C: NIH COMMENTS

DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

National Institutes of Health
Bethesda, Maryland 20892

www.nih.gov

DATE: August 8, 2025

TO: Carla J. Lewis
Acting Deputy Inspector General for Audit Services, HHS

FROM: Principal Deputy Director, National Institutes of Health

SUBJECT: NIH Comments on Draft Report: "*The National Institutes of Health Needs to Improve the Cybersecurity of the All of Us Research Program to Protect Participant Data*" (A-18-24-06111)

Attached are the National Institutes of Health's (NIH) comments on the Office of Inspector General's (OIG) draft report, "*The National Institutes of Health Needs to Improve the Cybersecurity of the All of Us Research Program to Protect Participant Data*" (A-18-24-06111).

NIH appreciates the review conducted by the OIG and the opportunity to provide clarifications on this draft report. If you have questions or concerns, please contact Meredith Stein in the Office of Management Assessment at 301-402-8482.

Matthew J. Memoli, M.D., M.S.

Attachments

GENERAL COMMENTS FROM THE NATIONAL INSTITUTES OF HEALTH ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF INSPECTOR GENERAL DRAFT REPORT ENTITLED – "THE NATIONAL INSTITUTES OF HEALTH NEEDS TO IMPROVE THE CYBERSECURITY OF THE ALL OF US RESEARCH PROGRAM TO PROTECT PARTICIPANT DATA" (A-18-18-06111)

The National Institutes of Health (NIH) appreciates the evaluation conducted by the Office of the Inspector General (OIG) and the opportunity to provide clarifications on this draft report. NIH respectfully submits the following general comments.

OIG Recommendation 1:
We recommend that NIH require the DRC awardee to implement access controls to prevent DRC and DRC-RW information systems users from accessing the systems while abroad without verified approval.

NIH Response:
NIH concurs with the OIG's recommendation and considers it closed-implemented.

The DRC has implemented processes to prevent any user from accessing the systems from countries of concern, in accordance with the guidance received from NIH consistent with EO 14117 and 28 CFR Part 202. The DRC has also implemented a robust process by which researcher users to the Research Workbench go through both institutional and individual vetting and authorization and receive credentials permitting access to the systems from inside the US or abroad (as long as they are not accessing them from countries of concern). In addition, the DRC has implemented processes for its verified internal users with privileged credentials to notify their intent in advance to access systems from abroad. Further, the DRC has alerts in place to identify when information systems users with privileged credentials access sensitive areas of the DRC and DRC-RW from outside the United States and are investigated by consulting the prior approval list. If the user is not on that list, an email is sent, and the user is disabled if there is no response within 24 hours. In addition, data egress alerts that monitor exfiltration are also in place.

OIG Recommendation 2:
We recommend that NIH require the DRC awardee to identify and implement a control or compensating control to prevent the downloading of detailed participant data, as required by the *All of Us Data Use Policies*.

NIH Response:
NIH concurs with OIG's recommendation and considers it open.

The program has implemented compensating controls from early in the program operations to minimize the impact of these actions while maintaining the ability for the researchers advancing science with *All of Us* data to download the results of their analyses that are needed to publish or otherwise disseminate their findings.

GENERAL COMMENTS FROM THE NATIONAL INSTITUTES OF HEALTH ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF INSPECTOR GENERAL DRAFT REPORT ENTITLED – "THE NATIONAL INSTITUTES OF HEALTH NEEDS TO IMPROVE THE CYBERSECURITY OF THE ALL OF US RESEARCH PROGRAM TO PROTECT PARTICIPANT DATA" (A-18-18-06111)

The DRC's compensating controls include:

1) A banner warning appears to the users prior to executing any download, alerting them that *All of Us* policies prohibit them from removing or distributing participant-level data from the RW. Users must check a box to confirm their understanding prior to executing the download.
2) The DRC has implemented tools and alerts for monitoring the volume and speed of data downloaded. If a large amount of data is downloaded in a short period of time, alerts are triggered to the awardee for action. Each egress event is individually investigated by the awardee's security team, which works to ensure that any inappropriately downloaded data are deleted from the user's device. Accounts are disabled after three egress attempts, as well as for researcher nonresponse, and are re-enabled only once the incidents are fully resolved. Repeat violations or evidence of malicious behavior would be sent to the RW oversight body for deliberation and further action as necessary.

The DRC and Program have explored alternatives and decided that the current posture is best suited to meet the Program's policies without creating undue barriers to research. The alternative that has been implemented in similar programs is airlocking the data. Given the cadre of researchers using *All of Us* data, this approach would stymie advancement, be cost prohibitive, and provide no measurable increase in participant privacy or security.

Additionally, all prospective data users are required to complete user training. This training reinforces the provisions of the Data User Code of Conduct and appropriate user behaviors, including security and privacy awareness, with specific emphasis on the ban on row-level downloads. At the end of the training, there is an evaluation, which researchers must pass in order to continue with the access process. Before gaining access to the data resources, researchers must sign the Data User Code of Conduct, signifying their promise to comply with the program's requirements. Both the user training and Code of Conduct attestation steps are required annually for researchers to retain their user credentials.

Noncompliance with the Code of Conduct and other program policies, including row-level data download, may result in termination of users' *All of Us* Research Program accounts and/or other sanctions, including, but not limited to:

- The posting of the researcher's name and affiliation on a publicly accessible list of violators,
- Notification of the National Institutes of Health or other federal agencies as to their actions, and
- Possible financial or legal repercussions.

GENERAL COMMENTS FROM THE NATIONAL INSTITUTES OF HEALTH ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF INSPECTOR GENERAL DRAFT REPORT ENTITLED – "THE NATIONAL INSTITUTES OF HEALTH NEEDS TO IMPROVE THE CYBERSECURITY OF THE ALL OF US RESEARCH PROGRAM TO PROTECT PARTICIPANT DATA" (A-18-18-06111)

NIH will conduct a review of the current posture of controls and compensating controls and plans to provide an update in our Management Decision within 180 days following the issuance of the OIG's final report.

OIG Recommendation 3:
We recommend that NIH formally communicate national security concerns related to maintaining genomic data to *All of Us* award recipients that use or maintain genomic data and require the implementation of the IT security and privacy controls to protect the storage, transmission, and processing of such data.

NIH Response:
NIH concurs with the OIG's recommendation and considers it closed-implemented.

NIH takes security very seriously, including confidentiality, integrity, and availability of genomic participant data, and has updated its practices around Controlled-Access Data Repositories to reflect this perspective. The *All of Us* Research Program has adopted practices consistent with these changes by program policy and plans to continue to do so as agency guidance and policy develop further.

On July 25, 2024, NIH implemented Update for Data Management and Access Practices Under the Genomic Data Sharing Policy with Guide Notice NOT-OD-24-157. In support of recent security directives, NIH has implemented a technical update to enhance security measures focused on protecting data provided by NIH Controlled-Access Data Repositories.

Specifically, as of April 4, 2025, NIH is prohibiting access to NIH Controlled-Access Data Repositories and associated data by institutions located in countries of concern. These countries include China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela, consistent with EO 14117 and 28 CFR Part 202. NIH has updated and formally communicated its implementation access practices consistent with Guide Notice NOT-OD-25-083 and plans to issue additional requirements in the future.

The *All of Us* Research Program's operations align with these changes, and the program will continue to work with agency policy and security leadership to ensure new expectations are met in a timely manner.

The above actions also align to Security Requirements for Restricted Transactions. These security requirements map to NIST SP 800-53, Moderate baseline. NIH selected the moderate baseline as deemed appropriate using NIST SP 800-60 Volume 2 latest revision: "Guide for Mapping Types of Information and Information Systems to Security Categories" and in alignment with CISA Security Requirements for Restricted Transactions. The excerpts below reflect this position:

GENERAL COMMENTS FROM THE NATIONAL INSTITUTES OF HEALTH ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF INSPECTOR GENERAL DRAFT REPORT ENTITLED – "THE NATIONAL INSTITUTES OF HEALTH NEEDS TO IMPROVE THE CYBERSECURITY OF THE ALL OF US RESEARCH PROGRAM TO PROTECT PARTICIPANT DATA" (A-18-18-06111)

> **See D.14.1 Access to Care Information Type** (Page 167)
> *Special Factors Affecting Confidentiality Impact Determination: Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPAA. The Privacy Act Information provisional impact levels are documented in the Personal Identity and Authentication information type. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management. In some cases, unauthorized disclosure of this information such as privacy-protected medical records can have serious consequences for agency operations.* ***In such cases, the confidentiality impact level may be moderate.***
>
> **See D.20.1 Research and Development Information Type**
>
> *Special Factors Affecting Confidentiality Impact Determination: Most research and development information is proprietary. Unauthorized disclosure of proprietary information violates several statures and Federal regulations (see Appendix E). Pre-publication disclosure or other unauthorized disclosure of research findings can have a serious adverse effect on agency operations, agency assets, or individuals.* ***In such cases, the confidentiality impact level associated with research and development is moderate.***

As instructed in OMB 17-02, Precision Medicine Initiative Privacy and Security, requirements for all Precision Medicine Initiative (PMI) Cohort Program partners, (later renamed to the *All of Us Research Program)*, outlined minimum security and privacy standards to be applied. These standards, commonly referred to at the PMI Data Security Policy Principles and Framework (2016) and Privacy Trust Principles (2016) were drafted by a White House Joint Task Force composed of leaders from HHS, DoD, DHS, and NIST. Both documents were derived from the NIST Cyber Security Framework (CSF). The OMB guidance did not require that PMI partners comply with FISMA since most of the data would not be considered federal. The NIH later committed to applying FISMA across the program, specifically the DRC/DRC-RW due to its sensitive nature. The NIH has consistently applied FISMA security controls since the inception of the program using the NIST Risk Management Framework, which requires a structured process for performing risk assessments on systems using a standard security control framework, such as NIST SP 800-53, Rev 5. This standard still exceeds that of most peer data repositories within NIH today. In addition, while voluntarily adopting the 800-53 standard, *All of Us* was on the front end of complying with the latest revision from NIST, Revision 5.

GENERAL COMMENTS FROM THE NATIONAL INSTITUTES OF HEALTH ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES OFFICE OF INSPECTOR GENERAL DRAFT REPORT ENTITLED – "THE NATIONAL INSTITUTES OF HEALTH NEEDS TO IMPROVE THE CYBERSECURITY OF THE ALL OF US RESEARCH PROGRAM TO PROTECT PARTICIPANT DATA" (A-18-18-06111)

OIG Recommendation 4:
We recommend that NIH require the DRC awardee to reevaluate the security categorization for the DRC and DRC-RW information systems considering the national security concerns of maintaining genomic data.

NIH Response:
NIH concurs with OIG's recommendation and considers it open.

The Program goes through a rigorous process to evaluate matters like this on an ongoing basis. The DRC is slated to renew its authority to operate in 2026 and this will be a key component of that evaluation that the Program anticipates beginning with the DRC awardee later this year.

NIH will provide an update on our timeline for this reevaluation in our Management Decision within 180 days following the issuance of the OIG's final report.

OIG Recommendation 5:
We recommend that NIH require the DRC awardee to update the remediation timeframe in its system security plans to comply with the timeframes specified in its award agreement with NIH.

NIH Response:
NIH concurs with OIG's recommendation and considers it closed-implemented.

The Program swiftly implemented the OIG's recommendation with the DRC awardee to create a milestone within their Plan of Action and Milestones (POA&M). NIH updated the System Security Plan language to align with the updated timeline in the award agreement. This milestone was completed, including signoff by the system owner, within 2 weeks of notifying the awardee of the finding. In addition, ongoing review of vulnerability timelines resulted in further refinement to the DRC security documentation in early August, reflecting the continuous improvement practices in place for security.

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov