1 EXECUTIVE SUMMARY

The Centers for Medicare & Medicaid Services (CMS) are permitted to disclose *Research Identifiable File (RIF)* data for research purposes. As part of this process, approved requesters of CMS *RIF* data enter into a Data Use Agreement (DUA) with CMS. As part of a DUA application, each organization completes a Data Management Plan Self-Attestation Questionnaire (DMP SAQ) to demonstrate compliance and preparedness with CMS security and privacy requirements.

The CMS Data Privacy Safeguard Program (DPSP) has reviewed the DMP SAQ of **The Curators of the University of Missouri (CUM).**This report is an analysis of the security exposure for CMS data that will be provided to **The Curators of the University of Missouri** for this DUA and study.

Organization	The Curators of the University of Missouri
Environment Name	Amazon AWS server instance
DMP Organization Name	CUM_AWS_030823
DPSP Rating	DPSP Review Complete DMP SAQ Approved
Approval Status	☒ **DMP SAQ Approved** ☐ DMP SAQ Not Approved
DPSP Review Date	March 08, 2023
DMP SAQ Expiration Date	April 06, 2024

The following are the key descriptors of the **Amazon AWS server instance** environment:

- **Physical Address:** US-EAST-2 (Ohio)
- **Shipping Address:** CE707 Clinical Support & Education Building, DC006.00, Columbia, MO 65212
- **Approved for Collaborator Use:** Yes
- **Cloud Technology:** Yes
- **Name they use to identify the Data Center:** Amazon AWS server instance
- **Data Custodian & POC for Data Center (Name, Phone & Email address):** Dr. Lemuel R. Waitman, 573-882-2190, russ.waitman@health.missouri.edu

- **Secondary POC (Name & Email address):** Dr. Xing Song, 573-884-0473, xsm7f@health.missouri.edu

2 SOURCES AND ATTESTATION EVIDENCE

DPSP based this report on the responses from the Data Management Plan Self-Attestation Questionnaire (DMP SAQ).

Policies and Documentation

The following policies were provided by **The Curators of the University of Missouri**, in the order shown, as evidence to support the attestation of the DMP SAQ responses:

1. Access Control
2. Awareness and Training
3. Audit and Accountability
4. Security Assessment and Authorization
5. Configuration Management
6. Contingency Planning
7. Identification and Authentication
8. Incident Response
9. Maintenance
10. Media Protection
11. Physical and Environmental Protection
12. Planning
13. Personnel Security
14. Risk Assessment
15. System and Services Acquisition
16. System and Communications Protection
17. System and Information Integrity

Additional Evidence was provided by the Curators of the University of Missouri as requested by the DPSP:

1. Workflow of account management (Administrative Workflow for Account Provision)
2. Screenshot of Review Invitation Email
3. Screenshot of Redcap Account Request Review Form
4. Screenshot of Jira Ticket for Account Creation
5. Annual grouse user review redcap form
6. Audit events on the information system including user logon and logoff (Baseline CloudWatch Events Enabled by Control Tower)
7. CloudTrail Console Example
8. CloudTrail Event with for all types of metadata
9. Screenshot of Metadata for a CloudTrail Event of "Console Login
10. Deny-all, permit-by-exception policy (screen shot of current User Groups)
11. CIS Benchmark Security Checks CIS 1.22 and CIS 1.16
12. Organization track, review, approve or disapprove, and log changes to organizational information systems (Change Management Workflow)
13. Confluence Documentation Version Control and Document Lifecycle Status

14. Established and enforced security configuration settings for information technology products employed in the organizational information systems (Security Hub Dashboard Example)
15. Authenticated identities of users, processes, or devices prior to granting access to organizational systems
16. Screenshot automated vulnerability scanner in compliance with DHS policies (AWS Inspector Scan Report as of 05/19/2021)
17. Screenshot of updated malicious code protection mechanisms (AWS Inspector Setup Screen in Management Console)
18. Monitor of organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks (Detective and Preventive controls relevant to tracking traffics) 19. Example of Security Hub Findings regarding Inbound and Outbound Traffic when not compliant
19. CloudWatch Event for unauthorized activity.
20. CloudWatch Log Stream view