UNM METALS Data Harmonization Web App: Use and Administration Policy

# Summary

This policy details the approved and unapproved uses of the UNM METALS Data Harmonization Web Application (app) at the UNM College of Pharmacy. The app has two functions. First, it facilitates the secure transfer and storage of harmonized datasets from partner institutions. Second, it allows approved users to conduct statistical analyses and produce graphics of summary data while limiting access to and visibility of raw data.

# Scope

## Stored Information

The following records are allowed in the app: de-identified records reporting laboratory analysis of detected metal concentrations in urine, blood, and serum, and term/preterm birth outcome data of biomedical study participants across cohorts. All data will be de-identified with random alphanumeric keys such that the geographic location and any other identifiable characteristics remain completely obscured within the app.

## Authentication

Access to the secure server where the web app is hosted is managed over a virtual private network (VPN) by UNMH IT via two-factor authentication using SecureLink.

## User Access

Password-protected access to the app and associated permission levels are authenticated through a user directory within the server. Levels of authorization to any dataset housed in the app are determined for each user depending on standing IRB protocols.

Because the app is used by researchers at partner institutions outside of UNM HSC, account registration is predicated on and limited to users who have access authenticated by UNMH IT through SecureLink.

## Monitoring

Monitoring occurs in two instances. First, SecureLink tracks and monitors who requests and is actively logged into the server over VPN. Access and user activities are monitored and recorded in Ubuntu log files and the Django Sentry monitoring package.

## Offboarding

In the event that a user no longer requires access to the app, the administrator will remove their access permissions from the user directory and will notify the UNMH SecureLink administrator.

## Training

Training on how to access the server and app has and continues to occur during regular project meetings with the partner institutions. SecureLink provides a comprehensive user manual upon access to the server. Documentation and service requests by users are maintained via GitHub.

## Data Backup and Recovery

All data are stored in an SQLite database within the app which is regularly inspected and backed up by the system administrator. However, individual datasets are owned and uploaded solely by research personnel named on the respective IRB protocols. As such, users are responsible for maintaining raw datasets. In the event that a revised dataset is uploaded to the app it completely overwrites older instances of the dataset.

Datasets can be completely removed using sudo controls within the Ubuntu server in which the app is maintained.

# Definitions

Administrator: Designated staff or faculty affiliated with the UNM Community Environmental Health Program – Data Management Core

Permission levels: Access to specific datasets as defined by IRB protocol to which those data are attached