Instructions

This document should be completed by the Unit Information Security Lead (UISL) or Unit IT Director. It will be reviewed by an ISO team member ("ISO Assessor") and the CISO.

The PI and/or researchers are responsible for providing data security requirements to the UISL or Unit IT Director.
The Unit IT Service Provider is responsible for determining and implementing technical solutions.

The technical solution must *meet or exceed* the UC IS-3 policy (https://policy.ucop.edu/doc/7000543/BFB-IS-3), UC Minimum Security Standard (https://security.ucop.edu/files/documents/policies/minimum-security-standard.pdf) and the standard required by the external party.

Each section contains either mandatory systemwide requirements or examples. Many of the mandatory systemwide requirements assume the data is classified at protection level 3.

Modify this plan as appropriate based on protection level, systemwide requirements and external party requirements.

If you have any questions regarding this form, contact infosecoffice@ucr.edu.

●

UNIVERSITY OF CALIFORNIA UC RIVERSIDE

Kurum Lab
Data Security Plan

Research Project Name:	Multilevel Time-Dynamic Modeling of Hospitalization and Survival in Patients on Dialysis
External Party:	USRDS
Principal Investigator(s):	Esra Kurum
Project Researcher(s):	Esra Kurum
Unit:	CNAS
Department:	Statistics
Unit IT Director or UISL:	Charles Forsyth
Unit Service Provider or IT Director:	Charles Forsyth
ISO Assessor:	Nick Christopher
CISO:	Dewight Kramer
Protection Level:	4
Availability Level:	2
Meets or Exceeds the Following Compliance Standards or Policies:	UC IS-3, UC Minimum Security Standard, USRDS Data Requirements, Appendix III to OMB Circular No. A-130
Date Approved:	

Revision History

Date	By	Contact Information	Description
1/26/2021	**Charles Forsyth**	**forsythc@ucr.edu**	**adding appendix, toc, and minor grammatical edits**
3/4/2021	**Charles Forsyth**	**forsythc@ucr.edu**	**Completed appendix, and adjusted signature section.**

3/18/2021	**Charles Forsyth**	**forsythc@ucr.edu**	**Added language around Crypto-Shredding.**

Executive Summary

The approved project researchers will have access to encrypted USRDS data folders stored on a secure server housed on the University of California, Riverside campus. All data will be viewed, modified, and utilized exclusively on the server itself over an encrypted network connection.

ALL storage and analysis of USRDS data will take place exclusively on the secure server. Data may not be downloaded to local workstations, or to any external devices, including laptops. Desktop and laptop workstations may be used only for remote access to the secure server.

Portable storage devices, including laptops, will not be used for downloading or storing data. USRDS data will NOT be shared with any other institution or any investigator not currently listed in this Data Security Plan. This restriction applies to source data as well as all derived data files. The project investigator, or designated project researcher, can modify researcher access to the USRDS data only after an approved modification and signing of the Data Security Plan.

All data security protections apply to the original USRDS data, derived files, and temporary analysis files.

Purpose

The purpose of this data security plan ("Plan") is to document the security measures and policies for handling data shared with the Principal Investigator ("PI") by USRDS. If this agreement is executed, all members of the research team with access to the data are contractually obligated to follow all aspects of the plan. The goal of the protections outlined in the plan is to prevent persons who are not signatories, or otherwise authorized, from gaining access to the data.

This plan applies to both raw data received, any copies of the raw data and any derivatives and output of analysis thereof.

Stakeholders, Roles, and Responsibilities

All stakeholders are responsible for reporting any suspected or confirmed incident or breach of data security to the PI, and ISO immediately.

- Principal Investigator (PI): lead researcher for Kurum Lab
    - Full access to the data on the secured analysis computer.
    - No administrative access to the secured analysis computer.

  - Responsible for supervising all research conducted using the data.
- UC Riverside Information Security Office (ISO): UC Riverside central information security office, under the direction of the Chief Information Security Officer (CISO).
  - No access to data.
  - No access to the secured analysis server.
  - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
- USRDS: Agency providing the data for the sole purpose of the investigation described in the USRDS data agreement.
  - Originator of data.
  - No access to the secured analysis server.
- Service Provider or IT Director/UISL: IT service provider responsible for provisioning, configuring, and managing the IT infrastructure used for processing the data.
  - Note: access described below will be limited to Research Computing staff members authorized by the Research Computing Associate Director.
  - Assists with PI for ensuring ongoing compliance with all elements of this plan.
  - Full access to data on the secured analysis server.
  - Administrative access to the secured analysis server.
  - Responsible for provisioning, deploying, and maintaining the IT environment for the secured analysis server.
- Project Researcher (Researcher): a researcher attached to the research project who will have access to the raw data under the direction of the PI.
  - Full access to data on the secured analysis server.
  - No administrative access to the secured analysis server.

Configuration of Secured Analysis Computer

Physical Access

- The secured analysis server will be physically located in 1348 Olmsted Hall on the UCR campus.
- The office is locked all times, except the time period accessed by authorized personnel.
- Only personnel authorized by the PI have access to the facility other than administrative staff.

Network Access Control

- The secured analysis server is behind the UCR Internet border firewall.
- The secured analysis server will only be accessible through SSH from a desktop or laptop.
- The secured workstation is on an ACL controlled an isolated network segment directly connected to the border firewall especially for P4 systems.
- The only outbound connectivity via the network segment would be for system patching and updates.

Encryption

- The secured analysis server will only be accessed via secure, encrypted communications protocols (SSH).

- Data will remain exclusively on the secure analysis server on encrypted storage.
- Data stored on the secured server will be encrypted using at least AES-128 encryption.

Access Management

- Non-administrative accounts will be created for each researcher with access to the secured analysis server.
- Only researchers who have signed this security plan will be granted accounts to access USRDS data.
- All accounts will be configured with passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf).

Logging and Auditing Configuration

- The secured analysis server is configured to store logs under normal log collection tools.
- OsSec is installed on the server server and provides a log filtering and alerting capability on the server. Allowing the server to alert the UISL and Pi in the case of malicious or wanted activity is found in the logs.
- Logs under the retained for at least 3 months.
- Logs are continuously reviewed for critical security issues.

Endpoint Protection

- Anti-virus protection is installed and configured with latest updates on desktops and laptops accessing the secure analysis server.
- Fire-eye and OsSec are installed on the secured analysis server.

Approved Applications

- In addition to the Linux operating system, associated system components, and system updates, Slurm Job Schedule, R and Matlab will be installed on the secure analysis server.

Transfer of Data from USRDS to UC Riverside

1. The United States Renal Data System (USRDS) Coordinating Center will provide the Requester data extracted from the USRDS research database (the “Data”), via download or on DVDs or other media types.
2. The Pi will upon approval, download the USRDS data via encrypted download link.
3. The transferred USRDS data will be stored on encrypted disks within the secure analysis server.

Operational Use of Secured Analysis Computer

- Only the PI and approved researchers will have access to the USRDS data on the secure analysis computer.
- No USRDS data sets will be copied from the secured analysis computer to any computer or device.
- Computation analysis will be conducted via the R software package and will remain exclusively on the secure analysis server.

- Derived works with P2 secure level can be downloaded to researchers laptops.

Cyclical Security Review

- Pi and UISL will be automatically alerted to anomalies in the logs from the secured analysis server, consisting of the elements described in the Logging and Auditing Configuration section above.
- Any deviations from the configuration specified in this plan or anomalies identified in the logs will be reported to the PI and UISL who will determine any required remediation and escalate any suspected security incident or breach to the ISO.

Log Review

- Secure server logs will be monitored by OsSec security software.
- Any anomalies and suspicious or unwanted log activity will be sent to the Service Provider or IT Director/UISL and the Pi for immediate review.

Vulnerability & Patch Management

- PI and authorized researchers will keep the operating system, antivirus/antimalware applications on the desktop or laptop that is used to access the secured analysis computer up to date.
- The Pi and Service Provider or IT Director will keep the operating system, system packages, antimalware and other security applications installed on the secure server up to date and controlled through regular patching.

Backup of Data

- Data or applications stored under the home directory on the secured analysis server are backed up daily to a secondary secure drive. Backups are retained for the entire time that is allowed and required in the data retention policy.

Data Retention & Destruction

- At the conclusion of the research period approved by USRDS, including any term extensions to the original agreement approved by USRDS, the data will be securely deleted from the secure analysis server using Crypto-shredding. Where the encryption key used to decrypt the data on disk is securely deleted. Preventing the encrypted data from being accessed or recovered ever again. The hard disks will then be securely formatted.

Security Plan Review

- This plan will be reviewed at least annually by the PI and UISL to verify continued compliance. Any risks identified will be added to the security plan following the process defined under Changes.
- During the review process, the PI will review the list of people with access to the data and ensure that access is revoked for any who no longer require access.

Violations of Data Security Plan

Any violations of the data security plan shall be reported immediately to the PI, UISL, Unit IT Director and CISO.

Security Plan Changes

Any changes to the IT environment or policies used for processing the data will be documented; approved by the PI and UISL; and submitted to the ISO for review and approval before implementation.

Agreement & Signatures

The undersigned agree to abide by this security plan.

Any researchers who will be granted access to the data covered by this plan in the future will be required to read and agree to the points above by signing an addendum to this plan.

Principal Investigator

Name: Esra Kurum

Signature: DocuSigned by:
8C90D132A7FD417...

Date: 3/19/2021 | 10:15 AM PDT

Unit IT Director/UISL

Name: Charles Forsyth

Signature: DocuSigned by:
Charles Forsyth
4C912C27FAE844D...

Date: 3/18/2021 | 4:12 PM PDT

Chief Information Security Officer

Name: Dewight F. Kramer

Signature: DocuSigned by:
Dewight F. Kramer
CE77FA9503B743A...

Date: 3/19/2021 | 4:28 PM PDT

Appendix

Requirement to Control Mapping

USRDS Data Requirements	
Requirement	**Control**
No copies or derivatives shall be made of the Data in these files except as necessary for the purpose authorized in this agreement.	● Data or applications stored under the home directory on the secured analysis server are backed up daily to a secondary secure drive. Backups are retained for the entire time that is allowed and required in the data retention policy. ● At the conclusion of the research period approved by USRDS, including any term extensions to the original agreement approved by USRDS, the data will be securely deleted from the secure analysis server using Crypto-shredding. Where the encryption key used to decrypt the data on disk is securely deleted. Preventing the encrypted data from being accessed or recovered ever again. The hard disks will then be securely formatted. ● No USRDS data sets will be copied from the secured analysis computer to any computer or device.
The Requester shall not publish or otherwise disclose the Data in the files to any person or organization unless the Data have been aggregated (that is, combined into groupings of Data such that the Data are no longer specific to any individuals within each grouping), and no cells (aggregates of Data) contain information on fewer than ten USRDS Agreement for Release of Data 2	● Only the PI and approved researchers will have access to the USRDS data on the secure analysis computer. ● No USRDS data sets will be copied from the secured analysis computer to any computer or device. ● Computation analysis will be conducted via the R software package and will remain exclusively on the secure analysis server.

individuals or fewer than five providers or facilities. The Requester shall not publish or otherwise disclose Data that identify individual providers or facilities, or from which such identities could be inferred. However, the Requester may release Data to a contractor for purposes of data processing or storage if (1) the Requester specified in the research plan submitted to the USRDS Project Officer that Data would be released to the particular contractor, or the Requester has obtained written authorization from the PO to release the Data to such contractor, and (2) the contractor has signed a data release agreement with the PO.	● Derived works with P2 secure level can be downloaded to researchers laptops.
Appropriate administrative, technical, procedural, and physical safeguards shall be established by the Requester to protect the confidentiality of the Data and to prevent unauthorized access to it. The safeguards shall provide a level of security outlined in OMB Circular No. A-130, Appendix III — Security of Federal Automated Information Resources, which sets forth guidelines for security plans for automated information systems in Federal agencies.	See Appendix:

Appendix III to OMB Circular No. A-130	
Requirement	**Control**
Assign Responsibility for Security	● Roles and Responsibilities are defined in this DSP's Stakeholders, Roles, and Responsibilities Section
System Security Plan	● This signed DSP.
Review of Security Controls	● Pi and UISL will be automatically alerted to anomalies in the logs from

	the secured analysis server, consisting of the elements described in the Logging and Auditing Configuration section above. ● Any deviations from the configuration specified in this plan or anomalies identified in the logs will be reported to the PI and UISL who will determine any required remediation and escalate any suspected security incident or breach to the ISO.
Authorize Processing	● Non-administrative accounts will be created for each researcher with access to the secured analysis server. ● Only researchers who have signed this security plan will be granted accounts to access USRDS data. ● All accounts will be configured with passwords meeting or exceeding the UC password strength standard (https://security.ucop.edu/files/documents/policies/account-and-authentication-management-standard.pdf).
Application Security Plan	● In addition to the Linux operating system, associated system components, and system updates, Slurm Job Schedule, R and Matlab will be installed on the secure analysis server. ● All Applications will be kept current with versions and security patches.