Data Security Plan

CRISPR_Gene_Editing_Research

Generated by Ursa DSP

2025-12-23

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").

The **Lab Director 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 following policies and standards: * UC IS-3 Policy * UC Minimum Security Standard * The standard required by the external party (e.g., UCSF Medical Center / HIPAA compliance)

The UC IS-3 policy requires all researchers to "develop and follow an information security plan that manages security risk over the course of their project."

Each section contains IS-3 requirements and example controls. Units should complete the controls to meet or exceed all data security requirements. Controls implemented to meet external party requirements should be listed in the appropriate rows.

If you have any questions regarding this form, contact the Information Security Office Risk Team at iso-risk@ucr.edu.

Research Project Data Security Plan

Research Project Name: CRISPR Gene Editing Research
External Party: UCSF Medical Center
Principal Investigator: Dr. Jennifer Doudna
Project Researcher(s): Dr. Jennifer Doudna, [List Additional Researchers]
Unit: Department of Molecular and Cell Biology
Department: Department of Molecular and Cell Biology
Unit Information Security Lead (UISL): [Name of UISL]
Unit IT Director: [Name of IT Director]
Unit Service Provider: [Name of Service Provider]
ISO Assessor: [Name of ISO Assessor]
CISO: [Name of CISO]
Protection Level: P4

Availability Level: A2
Meets or Exceeds the Following Compliance Standards or Policies: UC IS-3, UC Minimum Security Standard, HIPAA Security Rule
Date Approved: [Date]

Revision History

Date	By	Contact Information	Description
[Current Date]	Dr. Jennifer Doudna	[Email Address]	Initial Draft

Revision History

Date	By	Contact Information	Description
2024-05-21	Research Compliance Office	compliance@university.edu	Initial creation of Data Security Plan for CRISPR Gene Editing Research (HIPAA).

Table of Contents

Executive Summary

This research project, titled "CRISPR Gene Editing Research," is conducted by Principal Investigator Dr. Jennifer Doudna within the Department of Molecular and Cell Biology. The study utilizes sensitive patient data provided by the UCSF Medical Center, which is classified under the Health Insurance Portability and Accountability Act (HIPAA). To ensure strict compliance with HIPAA regulations and university security standards, the research team has implemented a hybrid infrastructure strategy.

Primary data storage and analysis occur on a secured local server, while redundant backups are maintained in a secure Cloud environment (AWS S3). Data transfer from UCSF is conducted exclusively via encrypted secure transfer methods (SFTP/HTTPS). Strict security controls, including encryption at rest and in transit, access control lists based on the principle of least privilege, and regular logging, are enforced to protect the confidentiality and integrity of the data.

All data associated with this project will be retained until the project's conclusion on December 31, 2026. Upon termination of the project, all data will be securely destroyed in accordance with NIST 800-88 Media Sanitization Guidelines.

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 the UCSF Medical Center. 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 Lab Director, UISL, and ISO immediately.

- **Principal Investigator (PI):** Dr. Jennifer Doudna, lead researcher for CRISPR Gene Editing Research.
  - Full access to the data on the secured analysis computer (Local Server) and AWS S3 backup.
  - No administrative access to the secured analysis computer.
  - Responsible for holding backup of data in escrow.
  - Responsible for supervising all research conducted using the data.
  - Shared responsibility with UISL for ensuring ongoing compliance with all elements of this plan.
- **Unit Information Security Lead (UISL) for Department of Molecular and Cell Biology:** [To Be Appointed/Identified], staff member appointed by the Dean of the Department of Molecular and Cell Biology with responsibility for information security.
  - Full access to data on the secured analysis computer.
  - Administrative access to the secured analysis computer.
  - Responsible for supervising Unit IT personnel with administrative access to the secured analysis computer and data.

- Shared responsibility with PI for ensuring ongoing compliance with all elements of this plan.

- **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 secured analysis computer.
  - Responsible for reviewing this plan, including approval of any future changes prior to implementation.
  - CISO is the responsible official for signing the data agreement with UCSF Medical Center. [NOTE: THIS IS ONLY THE CASE IF THE AGENCY REQUIRES IT, OTHERWISE IT IS THE PI.]

- **External Party:** UCSF Medical Center, agency providing the data for the sole purpose of the investigation described in the data agreement (Attachment 1: UCSF Data Sharing Agreement).
  - Originator of data (PHI).
  - No access to secured analysis computer.

- **Service Provider or IT Director for Department of Molecular and Cell Biology:** IT service provider responsible for provisioning, configuring, and managing the IT infrastructure (Local Server and AWS Cloud Infrastructure) used for processing the data, under the direction of the UISL.
  - Full access to data on the secured analysis computer.
  - Administrative access to the secured analysis computer.
  - Responsible for provisioning, deploying, and maintaining the IT environment for the secured analysis computer.

- **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 computer.
  - No administrative access to the secured analysis computer.

Configuration of Secured Computing and Storage

Configuration of Secured Computing and Storage

Access Control *Objective: Limit access to Institutional Information and IT Resources.*

UC Requirements (BFB-IS-3 Section 9)	Controls
Units must ensure that access to Institutional Information follows the Need to Know and Least Privilege principles.	**Local Linux Server:**• Access is restricted to the Principal Investigator (Dr. Jennifer Doudna) and authorized research staff listed in this plan.• User access is permitted only via the Campus VPN, which requires Multi-Factor Authentication (MFA).• Unique user accounts are provisioned for each researcher; no shared accounts are permitted.• SSH access requires key-based authentication; password-based SSH login is disabled.**AWS Cloud Infrastructure:**• Access to AWS resources (S3) is managed via AWS Identity and Access Management (IAM).• IAM policies enforce the Principle of Least Privilege, ensuring researchers only have access to specific buckets required for their work.• Root account access is secured with MFA and is not used for daily operations.
Units must limit access to authorized users and prevent unauthorized access to Institutional Information and IT Resources.	• Local server screens lock automatically after 15 minutes of inactivity.• Failed login attempts are monitored and will trigger a temporary lockout (Fail2Ban).

Encryption *Objective: Ensure appropriate access to protect UC Institutional Information and IT Resources.*

UC Requirements (BFB-IS-3 Section 10)	Controls
Units must encrypt Institutional Information classified at Protection Level 3 or higher when transmitted over a network.	• **Data in Transit:** All data transfers between the UCSF Medical Center, the local server, and AWS S3 will use secure protocols (SFTP, HTTPS/TLS 1.2+) to ensure end-to-end encryption.• SSH connections for server management utilize strong ciphers.

UC Requirements (BFB-IS-3 Section 10)	Controls
Units must encrypt Institutional Information classified at Protection Level 4 when stored on any electronic media.	• **Data at Rest (Local):** The local Linux server storage volumes utilize full-disk encryption (e.g., LUKS) using AES-256.• **Data at Rest (Cloud):** AWS S3 buckets are configured with Server-Side Encryption (SSE-S3 or SSE-KMS) using AES-256 to protect HIPAA data.• Encryption keys are managed securely and separated from the data where possible.

Physical and Environmental Security *Objective: Ensure appropriate physical access to protect UC IT Resources and Institutional Information.*

UC Requirements (BFB-IS-3 Section 11)	Controls
Units must implement and review physical security elements.	• **Local Server:** The server is physically located in a locked server room within the Department of Molecular and Cell Biology. Access to the room is restricted via key card logs to authorized IT and research staff only.• **Cloud Infrastructure:** AWS data centers are compliant with industry standards (SOC 2, ISO 27001). AWS is responsible for the physical security of the cloud infrastructure.
Units must ensure that physical access to secured areas is based on job responsibilities.	• Visitors to the local server room must be escorted at all times.• No HIPAA data is stored on portable media (USBs, external drives) unless explicitly authorized and encrypted.

Protection from Malware and Intrusion *Objective: Detect and prevent unauthorized access or malicious software.*

UC Requirements (BFB-IS-3 12.2)	Controls
Units must monitor IT Resources to detect signs of attack or compromise.	• **Local Server:** The Linux server runs an Endpoint Detection and Response (EDR) agent (e.g., Trellix HX or similar) and ClamAV for malware scanning.• Host-based intrusion detection systems (HIDS) are active.• **Cloud:** AWS GuardDuty is enabled to monitor for malicious activity and unauthorized behavior within the AWS environment.

Backup *Objective: Ensure data recoverability and retention compliance.*

UC Requirements (BFB-IS-3 12.3)	Controls
Units must ensure that Institutional Information classified at Availability Level 3 or higher is backed up and recoverable.	• **Strategy:** Primary data is stored on the local server with automated, encrypted backups replicated to a dedicated, versioned AWS S3 bucket.• **Encryption:** Backups in S3 are encrypted using AWS SSE.• **Retention:** Backups are retained in accordance with the project lifecycle (ending 2026-12-31) and HIPAA retention requirements.

Logging and Auditing *Objective: Record events and generate evidence for security monitoring.*

UC Requirements (BFB-IS-3 12.4)	Controls
Units must comply with the UC Event Logging Standard.	• **Local Server:** System logs (auth.log, syslog) are retained locally and forwarded to a centralized logging server (e.g., Splunk or Google Chronicle) where available. Logs are retained for a minimum of 6 years in compliance with HIPAA requirements.• **Cloud:** AWS CloudTrail is enabled to log all API calls and access to the S3 environment.• **Review:** Privileged account activity is reviewed periodically to ensure authorized use.

Control of Operational Software *Objective: Ensure only authorized software is used.*

UC Requirements (BFB-IS-3 12.5)	Controls
Units must obtain approval for software installation on production systems.	• Only software essential to the CRISPR research analysis (e.g., Python, R, specific bioinformatics tools) is installed.• Administrative access (sudo) is restricted to the Unit IT Director and designated Systems Administrators.• Unnecessary services and applications are disabled or removed.

Vulnerability & Patch Management *Objective: Maintain system security through updates.*

UC Requirements (BFB-IS-3 12.6)	Controls
Units must only use supported and patched versions of hardware and software.	• **Patching:** The local Linux OS is configured for automatic security updates. Critical patches are applied within 30 days of release.• **Scanning:** The Qualys Cloud Agent is installed on the local server to provide continuous vulnerability assessment.• AWS infrastructure is managed to ensure underlying services remain patched and supported.

Communications Security *Objective: Ensure the security of data in transit and network boundaries.*

UC Requirements (BFB-IS-3 Section 13)	Controls
Units must protect the ingress and egress points via appropriate network security controls.	• **Firewall:** The local server is protected by a host-based firewall (e.g., iptables/UFW) configured to deny all inbound traffic by default, allowing only SSH (Port 22) from the Campus VPN subnet.• **Cloud:** AWS Security Groups and Network ACLs restrict access to the S3 resources to authorized IP ranges only.• Unused ports and protocols are disabled.

Transfer of Data from [EXTERNAL PARTY] to UC Riverside

1. **Data Encryption:** Before being transmitted to UC Riverside, UCSF Medical Center will encrypt the data files (e.g., in ZIP format) using AES-256 encryption. The encryption passphrase shall be unique and meet UC password complexity standards (minimum 12 characters, mixed case, numbers, and special characters).
2. **Secure Transmission:** The encrypted data will be transferred using a secure method agreed upon by both parties, specifically Encrypted Secure Transfer via SFTP or HTTPS (TLS 1.2 or higher). Unencrypted transmission methods (e.g., standard email or FTP) are strictly prohibited for HIPAA data.
3. **Data Reception:** The Principal Investigator (PI) or authorized designee will download the encrypted data directly to the secured Linux server or the designated encrypted AWS S3 bucket. Data will not be downloaded to local workstations, laptops, or unencrypted portable media.

4. **Key Management:** The decryption key or passphrase for the file will be transmitted to the PI via a separate secure communication channel (e.g., verbal communication via telephone). The key will not be stored in the same logical directory or storage bucket as the encrypted data file.

5. **Decryption and Verification:** The authorized researcher will decrypt the file within the secured Linux environment. Upon confirmation of successful decryption and data integrity, the researcher will ensure the original transfer copy is securely deleted or archived according to the project's retention policy.

Operational Use of Secured Analysis Computer

Operational Use of Secured Analysis Computer

- **Authorized Access:** Only the Principal Investigator (Dr. Jennifer Doudna) and approved researchers listed in this Data Security Plan will have access to the Secured Analysis Computer and the associated data.
- **Data Ingress:** Protected Health Information (PHI) and research data provided by UCSF Medical Center will be transferred directly to the Secured Analysis Computer via Encrypted Secure Transfer (SFTP/HTTPS). No unencrypted transfer methods are permitted.
- **Data Storage and Backup:**
  - Active data will be stored on the local Linux-based Secured Analysis Computer in encrypted directories.
  - Backups of the original and working data sets will be securely transmitted to AWS S3 buckets configured with server-side encryption and strict identity and access management (IAM) policies. Access to backup repositories is restricted to the PI and authorized IT staff.
- **Data Egress:** Only aggregated, de-identified data and statistical analysis results will be copied from the Secured Analysis Computer for use in other applications, publications, or presentations.
- **File and Software Restrictions:**
  - Only statistical analysis scripts and approved applications necessary for the CRISPR Gene Editing Research project will be transferred to or installed on the Secured Analysis Computer.

    - No other data sets, applications, executables, documents, or personal files will be copied to or from the Secured Analysis Computer.
- **Exceptions:** Any operational need to remove un-aggregated, identifiable HIPAA data from the Secured Analysis Computer must be approved in advance by the PI and the Unit Information Security Lead (UISL).

Cyclical Security Review

At least once every three months, Service Provider personnel will perform a comprehensive security review and maintenance on the secured local Linux server and AWS cloud infrastructure used for the CRISPR Gene Editing Research project. This cyclical review is designed to ensure ongoing compliance with HIPAA standards and UC policies.

Maintenance Process and Tracking

The maintenance activities will be tracked as an **Incident record** in the UC Riverside ITS ServiceNow instance, including a completed checklist of all required actions. During this maintenance window, the local server's network interface may be temporarily re-enabled/connected via a NAT router/firewall to facilitate necessary updates; however, inbound access will remain blocked to prevent unauthorized access.

Required Review Actions

Service Provider personnel (including Systems Team and ISO as needed) will validate the following controls using this plan as a baseline:

- **Cloud Infrastructure (AWS):**
    - **IAM Access:** Audit AWS IAM roles and policies to ensure the principle of least privilege is maintained.
    - **Storage Security:** Verify AWS S3 bucket policies to ensure **Block Public Access** is enabled and default encryption (AES-256) is active for all backup data.
    - **Cloud Logs:** Review AWS CloudTrail logs to identify any unauthorized API calls or configuration changes.
- **Local Server (Linux):**
    - **System Logs:** Review system logs (e.g., `/var/log/auth.log`, `syslog`) for anomalies, specifically checking for unauthorized SSH access attempts or privilege escalation (sudo usage).

    - **File Integrity:** Compare file system audit logs for directories containing HIPAA data to verify that no accounts other than system accounts and approved researchers have accessed protected files.
    - **Malware Protection:** Review endpoint protection or antivirus logs (e.g., Trellix/ClamAV) to identify any malware threats.
    - **Patching:** Confirm that the OS and research applications are updated with the latest security patches.
- **User Access Verification:**
    - The PI (Dr. Jennifer Doudna) shall validate the current list of authorized users and permissions for both the local server and AWS environment.

Reporting and Remediation

Any deviations from the configuration specified in this plan or anomalies identified in the logs will be reported immediately to the PI and UISL, who will determine required remediation. Any suspected security incident or breach of HIPAA data will be escalated to the Information Security Office (ISO) immediately. At the completion of maintenance, the local server will be returned to its secure operational state.

Data Retention & Destruction

UC Requirement: When handling Institutional Information classified at Protection Level 3 or higher, Workforce Members may need to employ stronger methods of disposal at a more granular level to ensure that data is truly irretrievable. (Disposal of Institutional Information)

- At the conclusion of the research period approved by UCSF Medical Center (currently scheduled for 2026-12-31), including any term extensions to the original agreement, all HIPAA-regulated data will be securely deleted from UC Riverside systems and AWS infrastructure.
- **Local Server Sanitization:** The storage on the local Linux server will be sanitized using tools and methods compliant with **NIST 800-88 Media Sanitization Guidelines** (e.g., Clear, Purge, or Destroy techniques). If the hardware is to be decommissioned, physical destruction of the media will be performed.
- **Cloud Sanitization (AWS):** Data residing in AWS S3 will be deleted. To ensure data is truly irretrievable, the specific AWS KMS (Key Management Service) encryption keys used

to protect the S3 buckets will be securely deleted (Crypto-shredding), rendering any residual data unrecoverable.

- **Backups:** Any local backups or encrypted USB drives will be sanitized in accordance with NIST 800-88 standards. Cloud backups will be destroyed via the deletion of the associated encryption keys.
- **Audit Logs:** File access and security logs will be retained for six (6) years from the conclusion of the research period to comply with HIPAA retention requirements. After the retention period, logs will be securely destroyed.

Security Plan Review

This plan will be reviewed at least annually by the Principal Investigator (Dr. Jennifer Doudna) and the Unit Information Security Lead (UISL) to verify continued compliance with HIPAA regulations and university standards. Any risks identified will be added to the security plan following the process defined under Security Plan 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. This review specifically includes: * Validating physical access permissions to the local server. * Auditing logical access to AWS S3 storage buckets. * Verifying that only current, authorized personnel hold decryption keys for the UCSF Medical Center data.

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, architecture, or policies used for processing the data will be documented; approved by the Principal Investigator (PI) and Unit Information Security Lead (UISL); and submitted to the Information Security Office (ISO) for review and approval before implementation.

Any changes to the list of researchers with access to the CRISPR Gene Editing Research data will be reflected in this document as soon as the change is made. This includes the addition of the researcher to this document accompanied by their signature.

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 ,agree and sign this plan or an addendum to this plan.

Role	Name	Signature	Date
Principal Investigator	Dr. Jennifer Doudna		
Unit Information Security Lead (UISL)	[Insert Name]		
Chief Information Security Officer (CISO)	[Insert Name]		
Project Researcher	[Insert Name]		