DAISEY Security Policy Manual

Updated September 2019

Center for Public Partnerships and Research
University of Kansas
1617 St. Andrews Dr.
Lawrence, KS. 66047

Table of Contents

Section 1: Purpose of Policy Manual

The DAISEY team is committed to preventing, detecting, containing and correcting security violations in the system through creation, administration and oversight of DAISEY policies and procedures. This Security Policy Manual outlines how DAISEY complies with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

Policies in this manual apply to CPPR's interaction with DAISEY and specifically to CPPR staff involved with DAISEY. CPPR staff and other entities and individuals in contact with DAISEY are governed by additional applicable policies, including but not limited to: KU-IT Policies, KU Center for Research policies, Assessment and Achievement Institute Policies, and Center for Public Partnerships and Research policies.

DAISEY policies and this manual can be updated twice per year.

Section 2: Security Responsibility

2.1 Structure of Responsibilities
Purpose: Outline security and governance responsibilities and procedures related to protecting PHI in DAISEY.

Policy Statement: Multiple entities within the University of Kansas have responsibilities for DAISEY security. DAISEY is primarily designed, administered and supported by CPPR. CPPR manages organizations and initiatives within DAISEY, providing support, technical assistance and designing system infrastructure for each initiative. Agile Technology Solutions (ATS) provides technical development and operations of the system (e.g., programming and server management). KU Information Technology Services (KU IT) provides support and administration for the infrastructure providing the servers that DAISEY lives on.

Each organization has internal data governance for regular operations that include DAISEY projects. In addition, CPPR and ATS are part of the Achievement and Assessment Institute (AAI) and therefore have some degree of shared governance

2.2 DAISEY Management Team
Purpose: Identify the group responsible for making high level decisions regarding DAISEY.

Policy Statement: The DAISEY Management Team is responsible for making high level decisions regarding DAISEY. Members include the Associate Director of CPPR, DAISEY Security Officer, and the DAISEY Business Analysts.

This team will be responsible for ensuring that all PHI in electronic form is protected against reasonably anticipated threats or hazards to the security and integrity of PHI, and against reasonably anticipated improper uses and disclosures under the Privacy Rule.

2.3 DAISEY Security Officer

Purpose: Identify the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule.

Policy Statement: CPPR has designated a Security Officer who is responsible for the development and implementation of policies and procedures related to DAISEY as required by HIPAA.

2.4 DAISEY Security Governance Board
Purpose: Establish a governing body to ensure alignment of security strategy with DAISEY development and operations.

Policy Statement:
The Security Governance Board is a body responsible for reviewing security policies, providing guidance and feedback, and ensuring alignment with business objectives.

Members include the DAISEY Management Team, CPPR staff as appropriate, and representatives of ATS.

2.5 Feature Development

When CPPR staff are developing or enhancing features in the DAISEY system, security is a top priority. The ATS Development Team provides risk assessment information to the DAISEY Management Team during feature development and enhancements. Features that carry risk are reviewed by the Security Governance Board which provides guidance on feature implementation.

Section 3: System Availability & Emergency Operations

In the event of an emergency (for example fire, natural disaster, system failure, or vandalism), DAISEY is committed to protecting the availability, integrity and security of data. The most critical service that is provided as soon as possible in an emergency is access by the Operations and DAISEY Management Team to determine the impact the emergency had on the DAISEY system. Availability of DAISEY to Support Users, End Users and Developers is a secondary service that will be established only after the Operations and DAISEY Management Teams have determined it is safe to do so and that DAISEY will function appropriately.

3.1 Uptime

Purpose: Establish expectations for DAISEY application, data, and report availability for users.

Policy Statement: The expectation is that the DAISEY application and reports are available and accessible to users during business hours: 8 AM – 6 PM Central Time Mon-Fri, excluding University recognized holidays. System maintenance is typically performed as necessary on Thursdays, after 6pm.

Any unavailability during business hours exceeding fifteen minutes shall be considered an outage.

3.1.1 Planned Outages

Purpose: Establish expectations for planned system downtime.

Policy Statement: In case of planned work that will result in an outage, users of DAISEY are to be notified 24 hours in advance by CPPR staff. ATS will notify CPPR staff as far in advance as possible regarding any work that will result in an outage. Planned outages will typically be conducted on Thursdays, after 6pm.

3.1.2 Unplanned Outages

Purpose: Establish expectations for alerting users and resolving unplanned system outages.

Policy Statement: In case of an unplanned emergency, ATS will inform CPPR staff as soon as they become aware of an outage. CPPR staff will inform users as soon as they become aware of an outage. CPPR staff will work with their IT partners to restore the system to working state as soon as possible. ATS will provide DAISEY team with updates regarding the state of the system every 2 hours. CPPR staff will provide users with an update when the application becomes available.

3.2 Disaster Recovery

Purpose: Establish expectations for data loss and disaster recovery.

Policy Statement: If there is a loss of application and/or database, a backup and recovery policy is in place to recover the application and database within 24 hours, with a guarantee of no more than one hour of data loss.

3.3 Data Corruption

Purpose: Establish expectations for mitigating a data corruption situation.

Policy Statement: DAISEY backups are kept for 90 days. If data corruption is discovered within those 90 days, CPPR staff can, with the help of their IT partners, bring up a pre-corrupted version of the database in a separate environment to recover uncorrupted data.

3.4 Loss of Data Center
Purpose: Identify disaster recovery process in the event that the Data Center is lost.

Policy Statement: In the event that the Data Center is lost, database backups are executed nightly to AWS. This ensures no more than 24 hours of data loss. ATS will restore the application to the most current viable backup.

3.5 Data Backup
Purpose: Maintain retrievable exact copies of DAISEY data.

Policy Statement: Point-in-time logs are kept for 7 days. Database backups are executed nightly. Backups are kept at KU for 60 days. Backups are kept on AWS for 90 days. This ensures no more than an hour of data loss as long as ATS retains access to the DAISEY database server. If the DAISEY database server is lost before the dump is copied to the backup servers, there will be no more than 24 hours of data loss.

3.6 Emergency Server Operations
Purpose: In the event of an emergency that impacts server operations, KU IT will follow their internal Continuity of Operations Plan.

Policy Statement: In the event of an emergency that impacts server operations, KU IT will follow their internal Continuity of Operations Plan.

In the event that KU IT informs CPPR staff that the DAISEY system has gone down, a designee shall notify the DAISEY Management Team who will determine an appropriate response. This may include initiation of Emergency Mode, detailed in CPPR DAISEY Security Policy 3.7.

3.7 Emergency System Operations (Emergency Mode)
Purpose: Protect the security of the DAISEY system and all DAISEY data in the event of an emergency that is, or has the potential to, compromise the security of the system.

Policy Statement: In the event of an impending or existing emergency that is or may compromise the system, any member of the DAISEY Management Team may initiate DAISEY's Emergency Mode.

To initiate Emergency Mode, a member of the DAISEY Management Team shall send an urgent message to the entire DAISEY Management Team stating that they are initiating Emergency Mode.

Upon receipt of the urgent e-mail, a DAISEY Management Team designee shall alter the system permissions tree to stop access for all users except the Operations and DAISEY Management Teams. A DAISEY Management designee should ensure that all DAISEY users are notified that Emergency Mode has been initiated. The DAISEY Management Team designee will determine what, if any details about Emergency Mode are provided to users.

Emergency Mode ends upon consensus of the DAISEY Management Team and notification to the designee. Upon receipt of this notification, the designee will reinstate system permissions and ensure that all users are notified that regular operations have been reinstated.

3.7.1 Emergency Mode Test

Purpose: Ensure proper functionality of Emergency Mode to disable access for all users except the BA and Operations teams.

Policy Statement: A DAISEY Management designee shall test Emergency Mode procedures at least once per year. The DAISEY Management designee shall monitor and document the results of the test. The Security Governance Board shall review the results of the test and may determine any necessary changes to any relevant policies and procedures.

Section 4: Data Governance

4.1 Tiered Data Governance

Purpose: Identify the relationships between parties including initiative funding agencies, grantees, clients and CPPR and ensure compliance with applicable laws and regulations protecting data.

Policy Statement: CPPR will ensure that all contracts and agreements appropriately address data security given the relationship of CPPR to the initiative agency; the relationship of the initiative agency to its grantees, referred to herein as Participating Agencies (PAs); and status of the initiative agency and PAs as HIPAA and/or FERPA covered entities.

CPPR will maintain templates for all documents and may work with each initiative to tailor these documents so they are suitable for each initiative's purpose and unique needs.

At a minimum, each initiative shall have the following data governance documents in place before users are permitted access to live data in DAISEY:

Document Name	Parties	Purpose
CPPR Contract (including BAA or DSA if appropriate)	Initiative Agency and KUCR/CPPR	Establishes details of services provided to the initiative by CPPR. Provides guidance for establishing details of Terms of Use. If the initiative involves HIPAA covered entities, the BAA or DSA shall address all requirements of a Business Associates Agreement.
Terms of Use	Initiative Agency and all initiative PAs	Establishes requirement that Participating Agencies (PAs) agree to certain data security protocols. In addition, the document outlines what data will be entered into DAISEY, how it will be used and how it will be protected. If the initiative involves HIPAA and/or FERPA covered entities, the Terms of Use shall address all HIPAA and FERPA requirements.
DAISEY User Confidentiality and Data Security Agreement	Individual DAISEY users	Establishes requirement that DAISEY users keep DAISEY information confidential and meet expected data security practices. Users must electronically agree to terms upon first DAISEY login and annually thereafter.
Client Authorization / Notification of Information Use / additional language for Notice of Privacy Practices	Individuals receiving services from a PA	Informs individuals receiving services from PAs that their data will be captured in DAISEY. Note: HIPAA covered entities may determine their Notice of Privacy Practices adequately informs clients and an additional Notification is not necessary.

Initiatives with PAs sharing data in DAISEY shall have the following data governance documents in place before users are permitted access to live data in DAISEY:

Document Name	Parties	Purpose
Community Partner Memorandum of Agreement	All PAs within a given data sharing community	Establishes terms that all PAs within a data-sharing community agree to, regarding how DAISEY data may be used and how it will be protected. Note: CPPR may work with the initiative to develop a template, and PAs may revise the mutually agreed upon terms to fit the needs of their data-sharing community. CPPR shall not open data sharing in DAISEY until the initiative has approved the PAs signed Community Partner MOA.
Authorization for Release of Information	Individuals receiving services from a PA in a data sharing community	Documents consent of individuals receiving services from PAs to have their data shared with other PAs in the community. Note: this authorization is used in place of the Client Notification of Information Use document, not in addition to it.

4.2 Violation of Data Governance Agreements
Purpose: Establish general guidelines for responding to violations of Data Governance Agreements.

Policy Statement: If a user or PA violates the terms of a data governance document to which they are a party, the Initiative Lead, DAISEY Management Team and/or the Security Governance Board shall work with initiative representatives to conduct a formal or informal investigation and determine the appropriate response.

Response to violations will be determined on a case-by-case basis based on the information gathered in the investigation. Considerations may include:

- intent- whether the violation was intentional or accidental;
- relationship of the parties to the agreement that was violated; and
- nature and severity of the incident.

At a minimum, the response shall include a verbal warning and/or relevant training. Response to an egregious violation may include termination of an agreement and termination of a user or PA's access to DAISEY.

CPPR shall document the violation and the response. If the violation constitutes a security incident or breach, CPPR staff shall log it in the Security Incident Log as described in DAISEY Security Policy 8.4.

Section 5: User Access

5.1 Access Control
Purpose: Ensure that all individuals who have contact with DAISEY have only the most restricted/limited access required to perform their job duties.

Policy Statement: Individuals in contact with DAISEY shall be classified into one System Group based on the type of contact prescribed by their job duties (see DAISEY Security Policy 5.2) and shall be limited to the most restricted User Role(s) that allow completion of job duties (see DAISEY Security Policy 5.4).

5.2 System Groups
Purpose: Restrict access to data for individuals having approved contact with DAISEY.

Policy Statement: Individuals in contact with DAISEY shall be classified into one of five System Groups that restrict access to DAISEY environments. Individuals shall be classified in System Groups as follows:

System Group	Description	Data Access
Development Staff	Developers contracted with ATS to develop the technical specifications of the system.	Only de-identified data in the application with the exception of on-shore Development staff with access to identifiable data in application and database
Operations Staff	ATS staff managing system administration, operations and database administration.	No application access. All data in database.
DAISEY Management Team	CPPR staff acting as application administrators. These users require access to and administrative control over all areas of the application in order to carry out duties. This group is limited to only a few staff because of the high risk level associated with its access.	All data in application
Support Users	CPPR staff acting as administrators in one or more system initiatives. These users require administrative access to portions of the system in order to carry out duties.	Limited identifiable data in application
End Users	Individuals using the system for its intended purpose as a data aggregation and reporting tool. Additionally, this can be CPPR staff that do not belong to System Groups listed above. An example is evaluation staff members.	Limited identifiable data in application

5.3 Environment Restrictions

Purpose: Restrict access to data, especially Personally Identifying Information and Protected Health Information and promote system security and privacy by limiting individuals' contact with DAISEY to only the parts of the system necessary to perform their job duties.

Policy Statement: Access for individuals in contact with DAISEY shall be limited to only the system environments necessary to perform their job functions. Only individuals with authorization to access sensitive information shall be permitted access to the Production environment.

Access to environments shall be restricted based on an individual's need to access sensitive information to fulfill their job duties related to DAISEY as described below:

Environment	Access by Group	Data	Purpose
Local	Development	Contains fake data	Initiate development changes in DAISEY
Development	Development, DAISEY Management Team	Contains fake data	Continue developing system changes
Quality Assurance	Development, DAISEY Management Team	Contains fake data and static real data that has been de-identified	Testing by the development team.
Staging	Development, DAISEY Management Team, and Support Users (as needed)	Contains static real data that has been de-identified	Final testing by the Development and DAISEY Management Teams. Support Users may provide testing support.
Production - Sandbox	DAISEY Management Team, Support Users, End Users	Contains fake data	Testing and End User Training.
Production - Live	DAISEY Management Team, Support Users, End Users	Contains real, live, identifiable data	Administration by DAISEY Management Teams and Support Users. Use by partners.

5.4 User Roles

Purpose: Promote system integrity and data security by limiting individuals' access to data and features in DAISEY to only what is necessary to perform their job duties.

Policy Statement: DAISEY users shall be assigned to the role or roles with the most restricted access to data and functionality permitting completion of their job duties. End Users are prohibited from being assigned a System Administrator role.

Roles and associated permissions and data access are described in the table below. Users may be assigned "switch access" between multiple DAISEY Organizations/Grantees if deemed appropriate for their job duties.

Level	Role	Permissions			Accessible Data
		System Mgmt.*	Regular Functions**	Data Mgmt.***	
System	Administrator	Standard	Standard	Standard	All data for all Initiatives
Initiative	Administrator	Limited	Standard	Standard	All data for their assigned Initiative
	User	No Access	Standard	Standard	All data for their assigned Initiative
	Reviewer	No Access	No Access	Limited	Limited data for their assigned Initiative
Grantee	Administrator	Limited	Standard	Standard	All data under their assigned Grantee
	User	No Access	Standard	Standard	All data under their assigned Grantee
	Reviewer	No Access	No Access	Limited	Limited data under their assigned Grantee.
Organization	Program Administrator	No Access	Standard	Standard	All data for their assigned Organization
	Provider	No Access	Limited	Standard	All data for their assigned Organization or Program(s)

*System Management

Standard Access	Can create, edit, and delete users, organizations, programs, forms, questions, modules, and roles.	
Limited Access	Initiative Admin	Can create and edit users, organizations, programs, forms, questions, and modules. No role permissions. No delete permissions.
	Grantee Admin	Can create and edit users and organizations. No program, form, question, module, or role permissions. No delete permissions.
No Access	No access to system management functions.	

**Regular Functions

Standard Access	Can create, edit, and delete profiles and activities.
Limited Access	Can create and edit profiles and activities. Can only delete activities that have not been submitted.
No Access	No access to profile or environment functions.

***Data Management

Standard Access	Access to import, export, and reports.
Limited Access	Access to limited information in reports determined by initiative.
No Access	No access to data management functions.

5.5 Determining CPPR Staff User Roles
Purpose: Prescribe the user role authorization process for CPPR staff.

Policy Statement: Access rights for Development and Operations staff are fixed. Access rights for CPPR staff are flexible. The DAISEY Management Team, and ultimately a designee of the DAISEY Management Team, is responsible for ensuring that CPPR staff have the appropriate role and minimum level of access required to complete job duties.

The DAISEY Management Team may consider the following to determine appropriate access for CPPR staff:

- Do they require access to real data or just the training module?
- Do they require access to a single initiative or multiple initiatives?
- Do they require administrative privileges in one or more initiatives?
- Do they require access to the fix or staging environments?
- Do they require system administrative privileges?

As responsibilities of CPPR staff change, the DAISEY Management Team shall review their access permissions and appropriately change their access within five business days.

5.6 Access Establishment and Monitoring

5.6.1 Access Establishment for CPPR Staff
Purpose: Establish procedures for granting and editing CPPR staff user access.

Policy Statement: DAISEY Management Team access must be granted by the DAISEY Management Team. The DAISEY Management Team may edit their own access.

Initial access and access edits for the Development staff must be made by the DAISEY Management Team in staging and fix environments. Access edits for Development staff in the local, development, and QA environments may be made by the Development staff.

Initial access for Support Users must be granted by the DAISEY Management Team or designee. Support Users may edit their access to more restricted roles. The DAISEY Management Team or designee must edit Support Users' access to less restricted roles.

Access to DAISEY by any CPPR staff or KU employee may be terminated at any time for any reason by the Associate Director of CPPR.

5.6.1.1 Access Establishment for CPPR Staff in Tableau
Purpose: Establish procedures for granting and editing CPPR staff user access in Tableau Server.

Policy Statement: Only CPPR staff designated as Tableau Administrative staff shall have Administrator access in Tableau server. CPPR staff designated as Initiative Coordinators, Initiative Leads, and Training and TA staff may have access to create and edit users and user groups in Tableau.

5.6.2 Access Establishment for End Users
Purpose: Establish procedures for granting and editing End User access.

Policy Statement: End user access may be established and edited by Support Users or by the DAISEY Management Team. Access shall be granted to an End User only after the user agrees to the terms of the User Confidentiality and Data Security Agreement by clicking "Agree" upon their initial login and annually thereafter.

5.6.2.1 Access Establishment for End Users in Tableau
Purpose: Establish procedures for granting and editing User access to reports and underlying data in Tableau Server through DAISEY.

Policy Statement: DAISEY End Users shall only access reports and underlying data in Tableau through the DAISEY interface. CPPR staff shall create Tableau user groups that correspond with the Initiative-Grantee-Organization hierarchy and user roles for a given Initiative in DAISEY.

End Users shall not be given any of the following permissions in Tableau Server: Share Customized, Web Edit, Save, Download Workbook/Save As, Move, Delete, or Set Permissions.

5.6.3 Access Monitoring for CPPR Staff
Purpose: Ensure that CPPR staff access is regularly reviewed, monitored, and edited as necessary.

Policy Statement: The DAISEY Management Team or designee shall review CPPR staff access at least quarterly, and remove or modify access for any CPPR staff that is no longer necessary for current job duties.

5.6.4 Access Monitoring for End Users
Purpose: Ensure that DAISEY End User access is regularly reviewed, monitored, and edited as necessary.

Policy Statement: Support Users shall modify End User access upon request from the user's organization or the Initiative funder. Before granting any request for a modification other than inactivating a user, Support Users shall confirm the appropriateness of the change with the organization's Primary Contact or the Initiative funder if an organization's Primary Contact is unavailable.

The DAISEY system shall inactivate any account that has been inactive for 6 months. End Users whose accounts are inactivated for this reason must contact the DAISEY help desk for reactivation of their account.

Initiative Leads and/or Coordinators shall instruct organizations of their responsibility to notify the DAISEY help desk when a DAISEY user leaves their organization or changes roles within the organization and no longer requires access to DAISEY.

Initiative Leads shall request that organizations review a list of that organization's End Users at least annually.

5.7 Documentation of User Access

5.7.1 Review of CPPR DAISEY Team Access

Purpose: Track CPPR staff access permissions in DAISEY to accurately document current staff roles in the system and maintain a history of staff access and roles.

Policy Statement: DAISEY maintains a record of all active and inactive accounts. The DAISEY Management Team or designee shall review and update CPPR staff access in DAISEY at least quarterly. This review shall consist of confirming that CPPR staff still need access to all initiatives, grantees, organizations, and roles for which they have active accounts in DAISEY. The designee shall maintain a CPPR Staff Access Review log documenting these quarterly reviews. At a minimum, this log must include the date of the review.

Note: Documentation of Operations and Development Team Access is maintained by ATS.

5.7.2 Documentation of End User Access

Purpose: Track End User access permissions in DAISEY to accurately document current roles in the system and maintain a history of access and roles.

Policy Statement: Initiative Coordinators shall maintain an Initiative End User Access Log (aka User Tracker) which functions as a user audit report of End User access for each initiative. At a minimum, this log must include information about user role(s), organizations, and access start and end dates. Initiative End User Access logs should be kept up to date in real time, as user access changes are executed in DAISEY.

Initiative Coordinators shall confirm current access needs with all Initiative organizations at least annually.

5.7.3 Review of User Access Documentation

Purpose: Provide oversight to ensure that user logs are properly maintained and current.

Policy Statement: The DAISEY Security Governance Board shall confirm that logs are maintained and updated. This includes the CPPR Staff Access Review Log, the Operations and Development Team log, and all Initiative End User Logs.

The Security Governance Board may review access logs to ensure that logs are properly maintained and current as described in DAISEY Security Policy 2.3.

5.8 Inappropriate Usage Sanctions

5.8.1 CPPR Staff Inappropriate Usage Sanctions

Purpose: Outline potential sanctions that would constitute an appropriate response to CPPR staff inappropriate use of DAISEY or inappropriate access to data.

Policy Statement: As described in the CPPR Confidentiality and Data Security Agreement (Appendix D), violation of CPPR security measures may result in disciplinary action, including but not limited to, privilege revocation and/or suspension or termination.

In the event that CPPR staff violates any CPPR or DAISEY policy regarding DAISEY, the CPPR Associate Director and Director will consult to gather information and determine appropriate response to misuse, abuse or fraud involving DAISEY. All pertinent KU Human Resource policies and procedures will be followed.

Note: ATS staff, including all contractors, are subject to sanctions as described in ATS Policy.

5.8.2 End User Inappropriate Usage Sanctions
Purpose: Outline potential sanctions that would constitute an appropriate response to inappropriate use of DAISEY or inappropriate access to data by an end user.

Policy Statement: CPPR may terminate the DAISEY account of any end user who is found to have violated the DAISEY Confidentiality and Data Security Agreement.

If an End User is suspected to have violated the DAISEY Confidentiality and Data Security Agreement or inappropriately access data or abused their access to DAISEY in any way, the CPPR Initiative Lead and/or Management Team will work with Initiative representatives to investigate the violation and determine the appropriate response.

Section 6: Security Measures

6.1 Administrative Safeguards

6.1.1 Security Awareness Training
Purpose: Ensure that all CPPR staff receive appropriate training regarding data security and data handling.

Policy Statement: CPPR staff must complete the CPPR Data Security Training, HIPAA training, KU IT Security Awareness Training, Human Subject Research Training, and CPPR DAISEY Security Training prior to being granted access to the system and at least every three years.

Note: Policies describing required trainings for ATS staff are maintained by the ATS Security Officer.

6.1.2 Security Reminders

6.1.2.1 Security Reminders for CPPR staff
Purpose: Ensure that CPPR staff are reminded of critical security information and best practices.

Policy Statement: The DAISEY Security Officer or designee shall send reminders to CPPR staff at least every 6 months. This communication will include a reminder that staff are required to change their DAISEY password at least once every six months and may include any relevant data governance and/or security information.

6.1.2.2 Security Reminders for End Users
Purpose: Ensure that End Users are reminded of critical security information and best practices.

Policy Statement: DAISEY Support Users shall send periodic e-mails to DAISEY users that include data security reminders, tips and/or best practices. This information may be included with e-mails about system features and updates.

6.2 Technical Safeguards

6.2.1 Unique User Identification
Purpose: Limit DAISEY system and data access to only approved individuals and ensure that user actions within the system are linked to individual users.

Policy Statement: Each DAISEY user will be assigned a unique user name and password. Initiative Leads/Coordinators and/or Support Users will inform end users at the time of account creation that sharing their login information is prohibited.

6.2.1.1 Unique User Identification in Tableau
Purpose: Limit access to reports and underlying data to only approved individuals.

Policy Statement: Each DAISEY user will be assigned a unique user name and password in Tableau Server that is different than their password in DAISEY. CPPR staff shall assign users to appropriate user groups based on the users access (hierarchy and role) in DAISEY. This limits users to only the reports

and underlying data they have permission to see and forces users to login through the DAISEY interface rather than directly into Tableau.

6.2.2 Password Requirements
Purpose: Promote system security by enforcing regular password changes and rigorous password requirements.

Policy Statement: The DAISEY system shall require users to change their password every six months. Accounts for users who refuse to change their password at least every six months shall be inactivated. The DAISEY system shall not permit a user to reuse any of their 10 most recent passwords.

The DAISEY system shall only accept passwords of at least 8 characters with at least one upper case letter, one lower case letter, one number, and one symbol.

6.2.3 Automatic Logoff
Purpose: Promote data and system security by ending a user's session after 30 minutes of inactivity.

Policy Statement: The DAISEY system shall automatically log a user off after 30 minutes of inactivity.

6.2.4 Malicious Software
Purpose: Protect the DAISEY system from malicious software.

Policy Statement: CPPR staff shall follow KU IT Security Awareness procedures for robust password management as well as AAI policies regarding technology use. CPPR staff shall immediately report discovery or suspicion of malicious software to Support Users and the DAISEY Management Team.

6.2.5 Log-in Monitoring
Purpose: Protect the integrity of the DAISEY system by monitoring unauthorized access attempts and failed login attempts.

Policy Statement: The DAISEY system shall log failed login attempts. This log shall include user information and the timestamp of each unsuccessful attempt.

The DAISEY system shall warn users after three consecutive failed login attempts that two additional failed login attempts will result in the user being locked out of the system.

The DAISEY system shall automatically inactivate the account of a user after a fifth consecutive failed login attempt.

Note: Operations staff at ATS maintain an Access Report documenting incidents of attempted unauthorized access to the DAISEY system.

6.2.6 Audit Controls
Purpose: Promote system and data integrity by ensuring proper server controls.

Policy Statement: Operations staff shall ensure that all of DAISEY's servers and infrastructure are being maintained according to the technical safeguards outlined in this policy.

6.2.7 Person or Entity Authentication

Purpose: Ensure the user accessing DAISEY is who they claim to be.

Policy Statement: DAISEY authenticates users based on unique usernames and passwords.

6.2.8 Encryption

Purpose: Prevent improper modification of information, limiting damage that could be done if someone gains access to the server.

Policy Statement: All database backups are encrypted using asymmetric encryption keys of 256 bit or greater.

6.2.9 Transmission Control

Purpose: Prevent improper modification of information in transit, limiting damage that could be done if someone gains access to transmitted information.

Policy Statement: Operation staff shall ensure that data is encrypted during transmission using modern, secure encryption technologies.

6.3 Data and Equipment Controls

6.3.1 Data Alteration and Destruction

Purpose: Ensure the availability of data when unplanned alteration or deletion becomes necessary.

Policy Statement: The DAISEY Management team can determine that due to technical requirements of the DAISEY application, transactional database, and/or reporting database, data may need to be altered or destroyed outside of the application. If determined, the team will develop a plan with ATS and act accordingly. A notification will be sent to users if necessary. Before data is altered or destroyed outside of the application (i.e. directly in database) a special backup will be created by ATS to ensure recovery in case needed. The special backup will expire and/or be deleted within 90 days.

6.3.2 Equipment Disposal or Reuse

Purpose: Ensure the proper disposal and destruction of data before equipment disposal, recycling, or reuse.

Policy Statement: All KU owned equipment used to store PHI will be sanitized and/or disposed according to KU's Electronic Data Disposal Policy (https://policy.ku.edu/IT/data-disposal) using the processes documented in the KU Electronic Data Disposal Procedure (https://policy.ku.edu/IT/electronic-data-disposal-procedure).

Section 7: Physical Safeguards

7.1 Facility Access Controls
Purpose: To limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

Policy Statement: Facility access controls for the KU data center and server room can be found at https://policy.ku.edu/IT/data-center-standards#access, section C.

7.2 Access Control and Validation Procedures
Purpose: To control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

Policy Statement: Access control and validation procedures for the KU data center and server room can be found at https://policy.ku.edu/IT/data-center-standards#access, section C subsection 3.

7.3 Maintenance Records
Purpose: To document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

Policy Statement: Maintenance information for the KU data center and server room can be found at https://policy.ku.edu/IT/data-center-standards#access.

7.4 Workstation Use
Purpose: To specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Policy Statement: CPPR staff are required to complete a security awareness training upon hire and then a refresher annually. Additionally, a reminder of data security best practices is sent out at least once every six months.

7.5 Workstation Security
Purpose: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Policy Statement: All CPPR staff workstations are set up with a sign on that is unique to each user. All workstations are identified and logged by serial number with the staff member assigned.

CPPR staff shall abide by all policies governing their KU accounts including:

Personal accounts http://technology.ku.edu/personal-accounts
Departmental accounts https://technology.ku.edu/departmental-accounts
Sponsored temporary accounts http://technology.ku.edu/services/sponsored-temporary-accounts

CPPR staff shall abide by all policies governing workstation security including:

KU IT Security Policy http://policy.ku.edu/IT/info-technology-security-policy

Section 8: Security Incidents

8.1 Security Incident vs. Security Breach
Purpose: Describe the difference between security incidents and security breaches.

Policy Statement: CPPR staff shall consider a situation in which an individual is able to view, access, modify or delete information that they should not have the ability to view, access, modify or delete to be a security incident and respond appropriately as described in DAISEY Security Policy 6.2.

CPPR staff shall consider a situation in which there is any unauthorized acquisition, access, use or disclosure of PHI that compromises security or privacy of data, causing significant risk of financial, reputational or other harm to an individual to be a security breach and respond appropriately as described in DAISEY Security Policies 6.2 and 6.3.

All security breaches are security incidents, but not all security incidents rise to the level of security breaches.

8.2 Response to Security Incidents
Purpose: Ensure proper and consistent handling of security incidents.

Policy Statement: Any CPPR staff who becomes aware of a potential security incident shall *immediately* notify the DAISEY Management Team via e-mail. The members of the DAISEY Management Team shall conduct or delegate the following to assess the situation and determine the appropriate response:

1. Implementation of measures to stop the incident as quickly as feasible, if it is ongoing;
2. Collection of information about the incident, including but not limited to:
    - Date incident began and was resolved
    - Date CPPR staff became aware of incident
    - Data involved
    - Impacted organizations, initiatives and partners
    - Details of how CPPR staff responded to resolve the incident
    - Response to underlying system defects responsible for incident (if applicable)

Once sufficient information has been collected, the DAISEY Management Team shall 1) determine whether there was indeed a security incident, 2) determine if the incident was a breach and 3) determine an appropriate response. Appropriate responses may include changes to system functionality, policies, and/or procedures. If the security incident is determined to be a security breach, the Security Governance Board shall ensure that Notice of Security Incident Letters are sent in accordance with policy CPPR DAISEY Security Policy 8.3. The DAISEY Management Team shall notify the Security Governance Board of any security incident or breach and response.

8.3 Notice of Security Incident Letters
Purpose: Ensure proper notification to affected parties in the event of a security incident or breach.

Policy Statement: In the event of a security incident that the Security Governance Board determines to be a security breach, the Board shall send a Notice of Security Incident (NOSI) letter to all affected parties. If the security incident is not a breach, the CPPR Associate Director (or designee) may determine whether or not a NOSI letter should be sent to affected parties.

The NOSI letter shall contain all pertinent information gathered about the breach. Applicable governing and contractual agreements should be considered in determining relevant 'affected parties'.

8.4 Security Incident Log
Purpose: Strengthen security by tracking security incidents and conducting continuous quality improvement activities.

Policy Statement: A designee of the DAISEY Management Team shall maintain a log documenting DAISEY security incidents. At a minimum, this log shall include incident start and discovery dates, information gathered about the incident, internal and external communication regarding the incident, and any response to the incident.

The Security Governance Board shall review the security incident log annually as described in DAISEY Security Policy 2.1 in addition to reviewing incident-specific information within the log after each security incident. The Board shall use the Security Incident Log to identify areas of opportunity related to tightening security and adjust policies and procedures as necessary.

Section 9: Evaluation and Testing

9.1 Evaluation
Purpose: To perform a periodic technical and nontechnical evaluation based on the standard HIPAA Evaluation rule.

Policy Statement: The Security Governance Board arranges for or performs a periodic technical and nontechnical evaluation, based initially upon the standards implemented under the standard HIPAA Evaluation rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

9.2 Risk Analysis
Purpose: Monitor and respond to potential risks and vulnerabilities that may compromise confidentiality, integrity, and availability of information in the DAISEY system.

Policy Statement: The Security Governance Board conducts or arranges for an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of information in the DAISEY system. A security audit will be conducted at a minimum every three years or if it is deemed necessary by ATS or the DAISEY Management Team due to significant changes to the software application. The assessments will be logged in the DAISEY Security Task Calendar with date of completion and a detailed report regarding each security assessment will be kept on file for tracking purposes.

9.3 Risk Management
Purpose: Implement security measures sufficient to reduce risk and vulnerabilities to an appropriate level.

Policy Statement: The Security Governance Board reviews the risk analysis and evaluates business impact to decide upon appropriate security measures.

9.4 Application and Data Criticality Assessment
Purpose: Assess the relative criticality of specific applications and data in support of other contingency plan components.

Policy Statement: A plan for application and data criticality assessment and evaluation will be developed and reviewed by the Security Governance Board.

Appendix A: Definitions

Business Associate Agreement (BAA) - Under HIPAA, Covered Entities (CE) may disclose PHI to a Business Associate or permit the Business Associate to create or receive PHI on its behalf, in order to help the CE carry out its health care functions. If such disclosures are made, the unit must obtain prior satisfactory written assurances that the Business Associate will appropriately safeguard the information. These written assurances are called Business Associate Agreements. The HITECH Act of 2009 requires BAs to comply with certain aspects of HIPAA including the privacy and security rules.

Covered Entity (CE) - The term "covered entity" is a HIPAA term that refers to three specific groups, including health plans, health care clearinghouses, and health care providers that transmit health information electronically. Covered entities must comply with the HIPAA's privacy rule and security rule requirements for safeguarding the privacy and security of protected health information.

Data Sharing Agreement (DSA) - A data-sharing agreement explicitly documents what data are being shared and how the data can be used. This type of agreement is typically used with organizations that are not HIPAA CE's, however CPPR may establish a DSA with a CE if CPPR is not acting as a Business Associate in the relationship.

Data Use Agreement (DUA) – A legally binding agreement between two parties when confidential information is shared. The agreement specifies confidentiality requirements of the relevant legal authority, security safeguards and data use policies and procedures. The DUA serves both as a means of informing data users of these requirements and a means of obtaining their agreement to abide by the requirements.

Family Educational and Privacy Rights Act (FERPA) – The Educational Rights and Privacy Act of 1974 gives parents access to their child's educational records and generally requires that schools have written permission from a parent or student in order to release any information from a student's education record.

Health Insurance Portability and Accountability Act (HIPAA) - The Health Insurance Portability and Accountability Act of 1996 requires regulations protecting the privacy and security of certain health information.

Health Information Technology for Economic and Clinical Health (HITECH) Act – Part of the American Recovery and Reinvestment Act of 2009, HITECH adds regulation surrounding HIPAA. The most notable change is that HITECH requires BAs to comply with the Security and Privacy Rules of HIPAA which they were not previously required to do.

Limited Data Set (LDS) - A limited set of identifiable patient information as defined in HIPAA Privacy Regulations. This data set may be disclosed to an outside party without an individual's authorization if certain conditions are met: 1) The purpose for disclosure is for research, public health or health care operations. 2) The recipient signs a DUA.

Protected Health Information (PHI) - Any individually identifiable health information held by a CE. "Identifiable" refers not only to data that is explicitly linked to a particular individual (that's identified

information). It also includes health information with data items which reasonably could be expected to allow individual identification.

Personally Identifying Information (PII) - Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. HIPAA refers to this information as Individually Identifiable Health Information (IIHI).

Terms of Use – Conditions and obligations to which users must agree in order to use DAISEY. Typically terms of use are between a funder and their grantee as an addendum to their contract. CPPR creates and provides these forms to the funder.

Appendix B: DAISEY User Access Audit Logs

This log is used to create the DAISEY User Audit Report provided to the DAISEY Security Governance Board annually.

Initiative User Log Example

User ID	Full Name	Organization	Role	Access Granted	Access Ended
000-78	John Murphy	Initiative	Initiative Admin	8/1/2015	
000-02	Melissa Stewart	Initiative	Initiative Admin	10/1/2015	
000-46	Kelly Moore	Organization A	Initiative User	11/1/2015	
000-12	Brandon Taylor	Organization A	Provider	3/1/2016	9/1/2015
		Grantee 1	Reviewer	9/1/2016	
000-11	George Thomas	Organization B	Program Admin	12/1/2015	6/1/2016
		Grantee 1	Grantee User	6/1/2016	

CPPR Team Log Example

User ID	Full Name	Initiative	System Group	Access Granted	Access Ended
000-01	Henry Bowen	N/A	Business Analyst	3/1/2014	
000-02	Jennifer Kane	N/A	Business Analyst	3/1/2014	9/1/2015
000-67	Jessica Miller	KDHE	Support User	6/1/2015	6/1/2016
000-19	Mary Brown	KDHE	Support User	5/1/2015	
		KEHS	Support User	4/1/2015	
000-45	Joshua Smith, UI Contractor	N/A	Operations Staff	5/6/2015	6/6/2015

Appendix C: HIPAA - § 164.308(a)(8), Standard: Evaluation.

Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.

What this means:

The security rule requires covered entities to periodically conduct an evaluation of their security safeguards to demonstrate and document their compliance with the entity's security policy and the requirements of this subpart. Evaluation replaced the concept and terminology of "certification" in the proposed HIPAA Security Rule. No official or government certification or credentialing bodies for HIPAA Security compliance exist at date of the publication of the final Rule. Evaluation may therefore be done in-house or with the assistance of security and compliance experts.

Once the security policies and procedures are implemented with an appropriate level of risk of that security being breached, the covered entity cannot simply sit back. As the environment changes, risks change. It is the responsibility of the covered entities to conduct an evaluation. Covered entities must assess the need for a new evaluation based on changes to their security environment and operational changes or even regulatory changes since their last evaluation. For example, new technology adopted or responses to newly recognized risks to the security of their information.

An evaluation by an external entity is a business decision that is left to each Covered Entity or Business Associate. Evaluation is required under § 164.308(a)(8), but a Covered Entity or Business Associate may comply with this standard either by using its own workforce or an external accreditation agency, which would be acting as a business associate. External evaluation may be too costly an option for small entities.

To ensure comprehensive coverage in technical evaluation, testing should include both security functional (to ensure the system components are enforcing security policies correctly) and penetration testing (to provide a level of assurance that security controls guard against circumvention).

Appendix D: CPPR Confidentiality and Data Security Agreement

CONFIDENTIALITY AND DATA SECURITY AGREEMENT
University of Kansas Center for Public Partnerships and Research (CPPR)
1617 St. Andrews
Lawrence, KS 66047

This document must be read and signed by any CPPR employee as a condition of employment. Violation of this agreement is grounds for immediate dismissal.

Data Ownership. All data related to specific CPPR programs or projects are the property of CPPR and/or its clients, and the directors, staff, contractors, and graduate students have no independent right to the data. Furthermore, any data that is collected as part of a research activity within CPPR is also considered to be property of CPPR and/or the client sponsoring the research. Some projects may have specific data use policies. Those policies are outlined in the appropriate Data Governance Handbook per software application. Data use policies must be followed at all times.

Data may be requested for non-CPPR research purposes, but permission to obtain such data must be granted by the director of CPPR. A description of the purpose and planned use of the data should be provided. Such permission may be granted on a case by case basis as long as such data does not reveal any personally identifiable information (such as information that can be used to identify a client). Using CPPR data for non-CPPR purposes without explicit permission is grounds for dismissal.

Confidential Information. For purposes of this Agreement, **"Confidential Information"** means all data or information that is proprietary to CPPR and not known to the general public, whether in tangible or intangible form, in whatever medium provided, including, but not limited to: marketing strategies, development tools, databases, works-in-progress, financial information, or projections, operations, business plans and performance results relating to the past, present or future activities of CPPR, plans for products or services, proposals and project information. All of these examples should reasonably be recognized as confidential information.

In addition all data as related to an employee's jobs duties will be considered Confidential Information and shall be held in strict confidence and Employees of CPPR shall exercise a reasonable degree of care to prevent disclosure to others as is specified in the CPPR Data Management and Security Policy and Procedure Manual.

Employees will not disclose or divulge either directly or indirectly the Confidential Information to others unless first authorized to do so in writing by the director of CPPR. Employees will not reproduce the Confidential Information nor use this information for any purpose other than the performance of his/her duties for CPPR.

All individually identifiable information, including individual protected health information protected under HIPAA, shall be treated as confidential unless written permission is granted to share that identified information. All state and school assessment materials, student names, and related data are also confidential.

This agreement shall not supersede any project specific confidentiality or data security requirements established by a project contract and/or agreement, which may be subject to, but not limited to, HIPPA and/or FERPA compliance.

IP Ownership. All products and results of services belong to and shall be the exclusive property of CPPR and/or its clients. The undersigned acknowledges and agrees that the products and results of services (and all rights therein, including, without limitation, copyrights) belongs to and shall be the exclusive property of CPPR and/or its clients.

The undersigned hereby acknowledges that CPPR and/or its clients shall retain all right, title, and interest in all trademarks, trade dress, and good will that results from any use or offer to sell thereof.

In particular, the undersigned agrees to comply with the following procedures and standards:

1. Adhere to the attached CPPR Data Management and Security Policy and Procedure Manual.
2. Legitimate discussions of matters related to confidential information should not take place in any public place, including, but not limited to, hallways, restrooms, reception areas, etc.
3. All confidential information must be stored on the CPPR secure network directory or using disk or file encryption methods on a computer or device.
4. Confidential information should not be saved to personal computers or devices.
5. Confidential information may not be removed from the premises at any time, except for the purpose of shredding, or stored on non-secure storage mediums.
6. Employee will not reproduce the Confidential Information nor use this information for any purpose other than the performance of his/her duties for CPPR.
7. Unneeded notes, forms or draft reports that bear identifying data or other confidential information must be shredded.
8. Computer passwords and login information shall not to be shared with anyone.
9. Employees must report loss of a computer or device, password, any actual or attempted unauthorized access, and use or disclosure of confidential data to supervisor and to other University personnel or officials as required by the policies or procedures of the University.
10. Employees must follow the CPPR Policies and Procedures for each software application they work with at all times.
11. The obligations under this agreement will continue after the staff member or student has terminated his/her relationship with CPPR or the University. Upon termination, staff and students will immediately return any documents, computers and/or devices, and media containing confidential data to CPPR.

Any violation of CPPR or University policies and procedures may result in disciplinary action, including, but not limited to, privilege revocation and/or suspension or termination.

I have read the above Confidentiality and Data Security Agreement, I understand the intent and specific requirements of this Agreement, and I hereby verify that I will comply with all aspects of this Agreement.

Name (print)	Position at CPPR
Signature	Date

Appendix E: Version Log

January 2016: Policy Manual Released

January 2017: Added policies related to Tableau

July 2018: Updated policies based on internal and external audit and added Physical Safeguard section

January 2019: Updated usage errors and added the new Confidentiality and Data Security Agreement

September 2019: Aligned wording with IRIS manual, made some contextual changes, and restructured responsibilities