Security Policy Overview

Updated January 2019

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

Table of Contents

Section 1: Introduction

The University of Kansas Center for Public Partnerships and Research (CPPR) is working to build upon existing efforts and infrastructure to ensure Kansas can effectively coordinate, improve, and track outcomes for children, youth and families across the state. To this end, CPPR developed Data Application and Integration Solution for the Early Years (DAISEY), a web-based shared measurement tool. DAISEY integrates and consolidates data for the purposes of secure HIPAA compliant centralized data storage and single-source reporting. DAISEY provides the capacity to fulfill funder reporting requirements and provides access to data for reporting and analysis to improve practice and services to children and families.

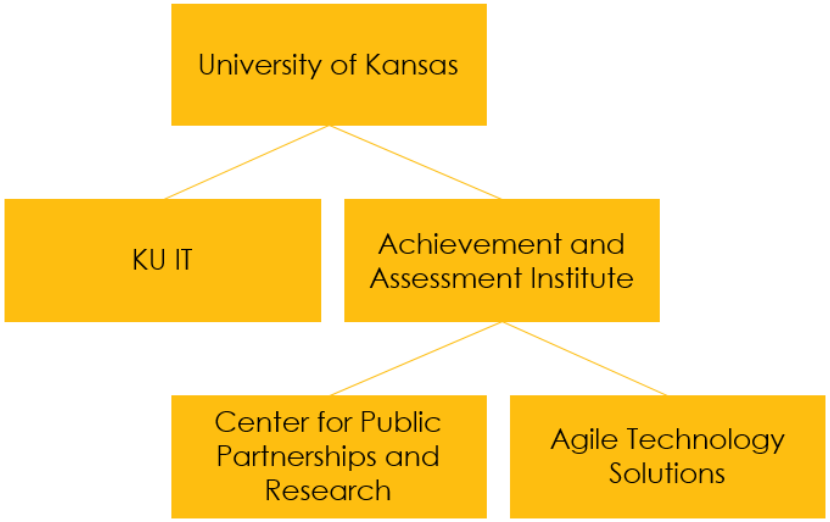
The DAISEY team is committed to preventing, detecting, containing and correcting security violations in the system through creation, administration and oversight of DAISEY policies and procedures. This overview of Data Security policies demonstrates the ways in which DAISEY complies with the Health Insurance Portability and Accountability Act (HIPAA), particularly the HIPAA Security Rule as well as the Family Educational Rights and Privacy Act (FERPA). This document describes robust administrative, technical, and physical safeguards of the DAISEY system and also provides contextual information to help readers understand the structure and governing policies of DAISEY

All policies referenced in this document are either publicly available or can be made available upon request.

Section 2: Security Responsibility

2.1 Structure of Responsibilities
Multiple entities within the University of Kansas have responsibilities for DAISEY security. DAISEY is primarily designed, administered and supported by the 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 (i.e. programming and technical infrastructure). KU Information Technology Services (KU IT) provides support and administration for 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.



In addition to the entities identified above, the University of Kansas Center for Research, Inc. (KUCR) is the KU entity that negotiates contracts on behalf of CPPR and ATS. KUCR reviews all DAISEY related contracts as well as security and privacy agreements that CPPR and/or ATS enter into. KUCR ensures that these documents are in compliance with applicable regulations and laws.

2.2 DAISEY Staff Groups
Because DAISEY operations are shared among numerous entities, there are some policies described in this document that apply to those entities differently. To differentiate which policies are applicable to DAISEY staff, this manual includes three staff groups.

- DAISEY Staff: All staff and contractors employed by AAI that work on DAISEY projects
- CPPR Staff: Employees of CPPR that work on DAISEY projects, all Business Analysts and Support Users
- Operations Staff: ATS staff responsible for DAISEY Operations
- Development Team: Developers working on DAISEY projects through contractual arrangements with ATS.

The DAISEY system is not open to all AAI staff. Rather, access is restricted to a limited number of AAI staff who work on DAISEY. AAI staff who do not work on DAISEY do not have access permissions for any part of the system.

2.3 DAISEY Management Team

The DAISEY Management Team is responsible for making high level decisions regarding DAISEY. Members include Associate Director of CPPR (Teri Garstka, PhD), and the DAISEY Business Analysts (Jared Barton, MSW, Joe Coburn, MSW, and Randi Harms, MA).

2.4 DAISEY Security Governance Board

The Security Governance Board is the governing body responsible for security of the DAISEY system. Members include the DAISEY Management Team, Director of ATS, CPPR Security Officer, and ATS Security Officer.

In addition to these individuals, an AAI staff member not working directly with or on a DAISEY project serves on the board to represent an external perspective. This person is selected by the CPPR Associate Director and serves voluntarily on the board. Other DAISEY staff participate in the board's functions as necessary.

The DAISEY Security Governance Board is responsible for

- development, communication and revision of security policies and procedures;
- review of periodic security evaluations and monitoring reports;
- review of security incidents and outcomes;
- addressing security concerns;
- accepting risk on behalf of DAISEY;
- arranging for or conducting risk assessments;
- monitoring changes to state and federal laws and other relevant regulation;
- informing IT security purchasing and investment decisions by CPPR and ATS that impact DAISEY;
- tracking IT industry standards to keep pace with improving tools and standards; and
- review and determination of special requests from funders that involve sensitive information or information that has been restricted by users as confidential.

The DAISEY Security Governance Board reviews various activity logs including the security incident log (Section 8.4), access report log (Section 6.2), and the user access audit log (Section 5.7).

The DAISEY Security Governance Board convenes twice per calendar year and as necessary to address security incidents or discuss system operations.

2.5 Feature Development

When DAISEY 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 CPPR Business Analyst team during feature development and enhancement. Features that carry risk are reviewed by the DAISEY 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 BA teams 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 BA teams have determined it is safe to do so and that DAISEY will function appropriately.

3.1 Uptime

The expectation is that DAISEY is available 24/7. DAISEY application and reports must be available and accessible to users during business hours: 8 AM – 6 PM Central Time Mon-Fri, excluding University recognized holidays. System maintenance is performed as necessary on Thursdays, after 6pm.

Planned Outages

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 prior regarding any work that will result in an outage. All planned outages will be conducted on Thursdays, after 6pm.

Unplanned Outages

In case of an unplanned emergency, ATS will inform DAISEY team as soon as they become aware of an outage. DAISEY team will inform users as soon as they become aware of an outage. DAISEY team 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. DAISEY team will provide users with an update when the application becomes available.

3.2 Disaster Recovery

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

DAISEY backups are kept for 90 days. If data corruption is discovered within those 90 days, DAISEY team 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

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

Exact copies of data are maintained by the ATS Operations staff. These backups are checked on a regular basis to ensure their availability in the event of an emergency. In the event of an emergency that causes data loss, ATS will utilize these backups to restore data to the DAISEY database.

In addition, KU IT will follow its Backup, Recovery and Archive Policy. This policy is not publicly available, however you may request a copy of the policy from the KU IT Security Office by submitting a form at https://technology.ku.edu/contact-it-security-office. Please reference the specific policy name listed here.

3.6 Emergency Server Operations
In the event of an emergency, KU IT follows its Continuity of Operations Plan in the event of an emergency. This policy is not publicly available, however you may request a copy of the policy from the KU IT Security Office by submitting a form at https://technology.ku.edu/contact-it-security-office. Please reference the specific policy name listed here.

In the event that KU IT informs DAISEY staff that the DAISEY system has gone down, the Lead BA will notify the DAISEY Management Team who will determine an appropriate response. This may include initiation of Emergency Mode, detailed below.

Emergency System Operations (Emergency Mode)
In the event of an impending or existing Emergency any member of the DAISEY Management Team may initiate DAISEY's Emergency Mode. The individual initiating emergency mode will do so by sending an urgent message to the Executive Team stating that they are initiating Emergency Mode.

Upon initiation of Emergency Mode by an Executive Team member, the Lead BA will alter the system permissions tree to stop access to all users except the BA and Operations team. The Lead BA (or designee) ensures that all DAISEY users are notified that Emergency Mode has been initiated. The Lead BA (or designee) will determine what, if any details about Emergency Mode are provided to users.

Any member of the DAISEY Management Team may end Emergency Mode by sending an urgent message to the entire DAISEY Management Team. Emergency Mode ends upon consensus of the Management Team. At that time the Lead BA (or designee) will reinstate system permissions and notify all users that regular operations have been reinstated.

Emergency Mode procedures are tested at least once per year. During that time emergency mode procedures are followed and monitored. The results of this test are reviewed by the Security Governance Board who will implement any necessary changes to policies and procedures.

Emergency Mode Test

The Lead BA (or designee) shall test Emergency Mode procedures at least once per year. The Lead BA 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 Documents

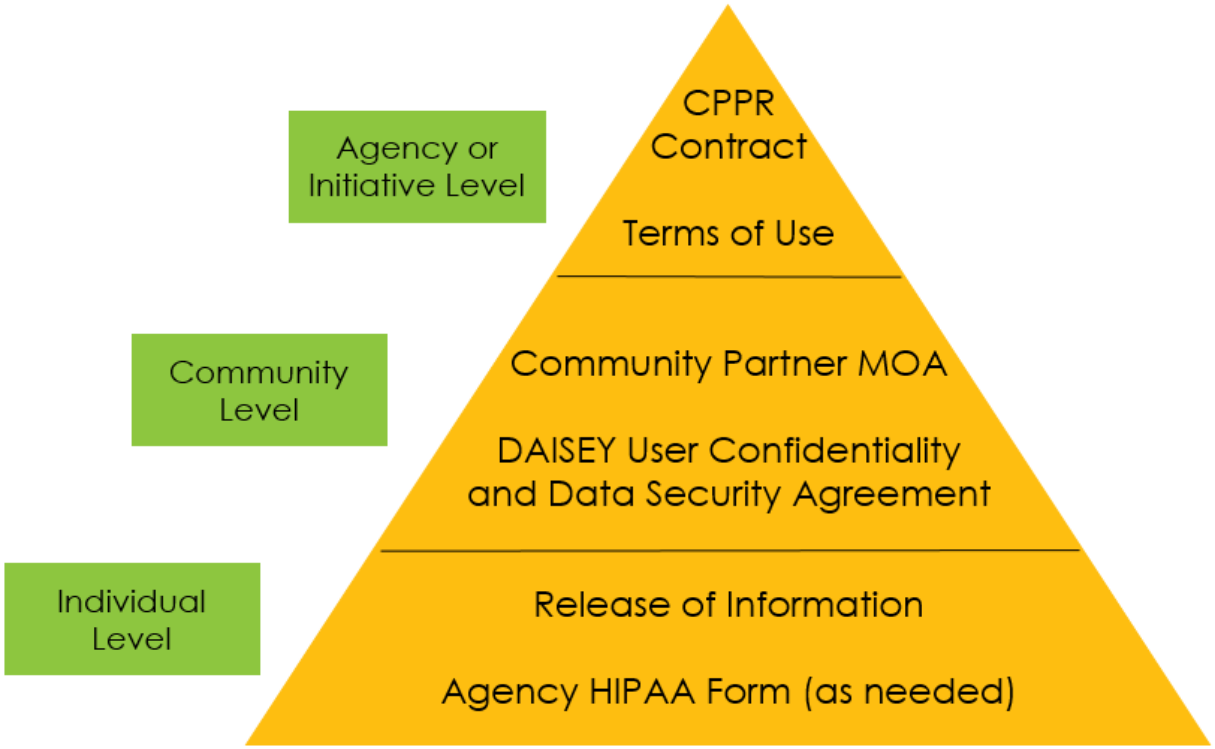
4.1 Tiered Data Governance

Because DAISEY deals with very sensitive data, the DAISEY team recognizes the need for thorough data security compliance. In order to ensure the highest level of data security for our partners, there are three tiers of documents and agreements that all DAISEY initiatives require. CPPR maintains templates for all documents and may work with initiatives to tailor these documents so they are suitable for each initiative's purpose.

1. Agency/Initiative Level
   The highest tier of documents are at the highest organizational level, between the initiative and CPPR or the initiative and its Participating Agencies (PAs). These documents inform language and terms in all other DAISEY documents.

2. Community Level
   The middle tier of documents is focused at the community level. Documents in this tier are between PAs within a community or completed by PA staff.

3. Individual Level
   The lower tier of documents is focused on individuals receiving services. This tier ensures those individuals are appropriately informed before their data is entered into DAISEY and shared.



DAISEY Data Governance Document Table

Document Name	Parties	Purpose
KU-CPPR Contract (including BAA or DSA if appropriate)	Initiative Agency and KUCR/CPPR	Establishes details of services provided to the initiative by KU-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: KU-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. KU-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

In the unfortunate circumstance that a user or organization/program violates the Confidentiality Agreement, Memorandum of Agreement, or Terms of Use, disciplinary action may be required. Final decisions regarding the appropriate response to a violation rest with the initiative. Based on the severity of the violation, the following may be considered potentially appropriate responses.

User Confidentiality Agreement

Staff of any partnering organization/program who discover a possible violation of the User Confidentiality Agreement, should notify the Initiative immediately.

Disciplinary action may be necessary if it is determined that a user has violated the User Confidentiality Agreement by:

1. Failing to comply with or violating relevant Terms of Use Agreement, MOA and Contract Agreements of their organization;
2. Sharing their login information with another individual;
3. Failing to immediately report loss of a password, actual or attempted unauthorized access, use to disclosure of PII/PHI to DAISEY Admin;
4. Failing to follow all federal, state and local laws and regulations applicable to collection, sharing and distribution of data;
5. Failing to follow the DAISEY Individual Data Sharing Declined Protocol;
6. Otherwise misusing DAISEY data or failing to ensure protection of the data.

In considering the appropriate response, the Initiative may investigate the nature, intent and severity of the violation. The Initiative may wish to align its response with its agency code of conduct policies. Appropriate responses might include, but are not limited to:

- Verbal warning
- Written warning
- Written reprimand
- Termination

Memorandum of Agreement or Terms of Use Agreement

Action may be necessary if it is determined that an organization or program has violated the Memorandum of Agreement or the Terms of Use by:

1. Failing to comply with all requirements of the Terms, MOA and Contract with KDHE;
2. Failing to ensure that all employees with access to DAISEY understand and acknowledge the confidentiality of program data, and the trust and confidence KDHE and partner organizations have placed in them by providing access to and contact with this information;
3. Failing to exercise diligence to protect and safeguard confidential and proprietary information as well as personally identifiable client level information;
4. Failing to notify all PAs within the agreement and KDHE within 10 days upon discovering any breach or suspected breach of security or of any disclosure of the data to any unauthorized individual or entity;
5. Failing to notify any other PA whose DAISEY data is used for scholarly research and analysis or professional presentation purposes, and/or failing to include the disclaimer on reports, presentations or other materials produced using DAISEY data;

6. Using or accessing the data for purposes other than those specified in the Terms of Use Agreement or MOA.

In considering the appropriate response, the Initiative may investigate the nature, intent and severity of the violation. Appropriate responses might include, but are not limited to:

- Verbal Warning
- Written Warning
- Terminating the offending organization/program from either or both Agreements

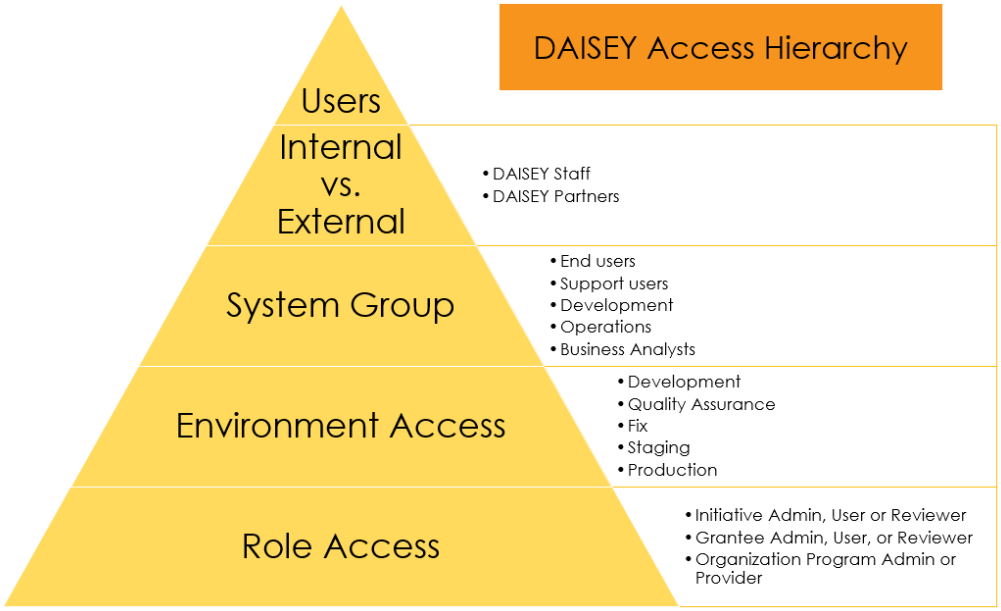
Section 5: User Access

5.1 Access Control
DAISEY relies on two role-based access controls for all users.

- DAISEY System Groups (Section 5.2)
  DAISEY users are classified into one of five system groups that restrict access to DAISEY environments within the application.

- DAISEY User Roles (Section 5.4)
  User roles classify DAISEY users into one of nine roles that restricts access to information within a given DAISEY environment.

A DAISEY user can be in only one *system group* but may have multiple *user roles*.



5.2 System Groups

DAISEY users are classified into one of five system groups that restrict access to DAISEY environments within the application.

System Group	Description	Data Access
Development Staff	Developers contracted with ATS to develop the technical specifications of the system.	Only deidentified data in the application with the exception of one on-shore Development staff with access to identifiable data in application and database
Operations Staff	ATS staff managing the technical requirements of system operation, primarily database administration.	No application access. All data in database.
Business Analysts (aka System Administrators)	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. Some end users have limited administrative permissions (e.g. the ability to adjust the hierarchy below their organization).	Limited identifiable data in application

5.3 Environment Restrictions

DAISEY Environments are versions of the DAISEY system that are established for various purposes. Access to these various environments is an aspect of DAISEY System Group access restrictions.

Environment	Access by Group	Data	Purpose
Local	Development	Contains fake data	Initiate development changes in DAISEY
Development	Development, BA	Contains fake data	Continue developing system changes
Quality Assurance	Development, BA	Contains fake data and static real data that has been deidentified	Testing by the development team.
Fix	Development, BA, and Support Users (as needed)	Contains fake data and static real data that has been deidentified	Testing by the development and BA teams. Support users may provide testing support to BA team.
Staging	Development, BA, and Support Users (as needed)	Contains static real data that has been deidentified	Final testing by the BA and development teams. Support users may provide testing support to BA team.
Production	BA, Support Users, End Users	Contains real, live, identifiable data	Administration by BA team and Support Users. Use by partners.

Environments are one of the ways that DAISEY ensures that all sensitive information, including PHI, is kept secure. Production is the only environment that contains identifying information. Only DAISEY staff authorized to access sensitive information are permitted access to the Production environment. DAISEY staff who are unauthorized to access sensitive information work only in environments that do not contain identifying information.

Production and Fix are the only environments available outside of KU's firewall. The remaining environments are only available through KU's Secure Virtual Private Network. Because Production is available outside KU's firewall, extensive protections are built into the environment to balance data availability and security.

In addition to these testing environments, Production contains a testing module that contains only fake information. The testing module is intended to provide users with a sandbox in which they can train and learn the system without risk to the integrity of data. Users are prohibited from entering real data into the training module. There are two safeguards that ensure the testing module does not prompt data incidents. First, user ids, names and dates of birth are removed from the testing module once per month. Second, users are reminded that they are prohibited from entering real data into the training module in four different ways. The DAISEY Confidentiality and Data Security Agreement (Appendix 3) states the prohibition, users are reminded when they receive user account information, trainers remind users during training events and a notice is posted on the module home page. These safeguards aim to prevent and minimize risk to DAISEY data.

5.4 User Roles

User roles classify DAISEY users into one of nine roles that restricts access to information within a given DAISEY environment.

A variety of user roles are available to meet the needs of initiatives using DAISEY. The primary purpose of each role is to provide appropriate access to a user based on their needs and responsibilities within an initiative. For example a direct service provider should not see the same information in DAISEY that an initiative executive should.

The chart below demonstrates the hierarchy of DAISEY user roles. The permissions for each role listed in this chart are the maximum permissions a user with that role may be allowed. Depending on initiative requirements, these roles may be further restricted. Roles may not have their permission expanded. If a user requires additional permissions, their role is changed to accommodate their needs. Support Users and End Users are prohibited from being assigned a System Administrator role.

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	Aggregate data for their assigned initiative. Generally restricted to aggregated data.
Grantee	Administrator	Limited	Standard	Standard	All data for organizations under their assigned grantee
	User	No Access	Standard	Standard	All data for organizations under their assigned grantee
	Reviewer	No Access	No Access	Limited	Aggregate data for organizations under their assigned initiative.
Organization	Program Administrator	No Access	Standard	Standard	All data for their assigned organization
	Provider	No Access	Limited	Standard	All data for their assigned organization. May be restricted to one or more programs.

*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. Cannot delete an activity unless it has been submitted.
No Access	No access to profile or environment functions.

***Data Management

Standard Access	Access to import, export and intelligent reports.
Limited Access	Access to import and export. Access to aggregate information only in reports.
No Access	No access to data management functions.

5.5 Determining DAISEY Staff User Roles

Appropriate roles and levels of access for DAISEY staff are determined based on job duties. Access is restricted in that DAISEY staff are given minimal access required to complete their duties.

Access rights for development and operations staff are fixed. Access rights for CPPR staff are flexible. The Lead BA considers the following to determine minimum access appropriate for CPPR staff:

- Do they require access to real data or just the training module?
- Do they require access only 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?

If responsibilities of a DAISEY staff change, their access permissions are reviewed and appropriately changed within five business days. Depending on the situation, the individual's access may be broadened, narrowed, or removed entirely. The Lead BA is responsible for ensuring CPPR staff have appropriate access. The ATS Director is responsible for ensuring Operations staff and the Development Team have appropriate access.

5.6 Access Establishment

DAISEY Staff

The Lead BA creates BA access. The BA team edits their own access; creates and edits Development team access in the staging and fix environments; and creates and edits Support User access. The development team edits their own access in the local, development and QA environments. Support Users create and edit End User access in the Production environment.

CPPR staff access can vary widely by duties and change regularly. To ensure access matches current duties, staff access rights are reviewed every three months by the Lead BA. Any access that is no longer required for job duties is removed at that time.

Only DAISEY staff designated as Tableau Administrative staff shall have Server Administrator access in Tableau server. DAISEY staff designated as Initiative Coordinators, Initiative Leads, and Training and TA staff may have Site Administrator access to create and edit users and user groups in Tableau.

End Users

DAISEY End users must submit a signed Confidentiality and Security Agreement (Appendix D) before their user account is created. Users whose accounts were created before this policy was implemented will submit a signed Confidentiality and Security Agreement by December 31, 2015.

A new process for completing user agreements is under development and will be implemented when ready. In the new process, the first time a DAISEY User logs in, they are prompted to accept the DAISEY Confidentiality and Security Agreement. Users reaffirm this agreement once per year. DAISEY logs acceptance of these agreements for documentation purposes.

DAISEY end users access reports and underlying data in Tableau Server through a single-sign-on in DAISEY. DAISEY end users access to reports and data in Tableau is consistent with their user role in DAISEY. End users are not given permissions to alter or save changes to reports on Tableau Server.

5.7 Documentation of User Access

The DAISEY Security Governance Board reviews access logs annually and in the event of a security incident. This includes three User Access Audit Logs which document individuals with access to DAISEY.

1. CPPR Staff Access
   The Lead BA (or designee) reviews CPPR staff access in DAISEY quarterly, making updates as necessary, and maintains a DAISEY Staff Access Review log documenting this review. The review ensures that staff only maintain access to various initiatives, grantees, and organizations if they still need it.

2. Operations and Development Team Log
   The ATS Security Officer maintains a user audit report for the operations and development teams. This report describes each staff's user role/access level and start and end dates of access.

3. Initiative User Log
   Maintained by Support Users acting as DAISEY initiative leads or coordinators, this log

documents individuals and organizations with user accounts in each DAISEY initiative. This report includes user role(s), organizations and access start and end dates.

Appendix B contains templates of these report logs.

5.8 Sanction Policy

Any DAISEY end user that fails to comply with established security policies is subject to relevant sanction policies. According to the DAISEY User Confidentiality and Data Security Agreement, violation of the agreement is grounds for termination of an individual's DAISEY account. KU is not responsible for enforcing applicable sanctions from the user's organization or funder.

Any DAISEY staff that fails to comply with established security policies is subject to relevant sanction policies. Applicable policies and procedures for sanction are determined by the DAISEY entity that has authority over a given staff:

CPPR

CPPR will apply penalties to CPPR staff who fail to comply with established security policies and procedures. CPPR staff are notified of this sanction policy during the required CPPR DAISEY Security Training.

As described in the CPPR Confidentiality and Data Security Agreement (Appendix C), 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 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.

ATS

ATS will apply penalties to staff who fail to comply with established security policies and procedures. Operations Staff are notified of this sanction policy during the required ATS Security Training.

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

ATS will apply penalties to contractors who fail to comply with established security policies and procedures. In the event that a Development team member violates any ATS policy regarding DAISEY, the ATS Director will gather information and determine the appropriate response that complies with contractual arrangements.

Section 6: Security Measures

6.1 Administrative Safeguards

Security Awareness Training and Reminders
All DAISEY staff are required to undergo training relevant to the work they do in DAISEY.

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.

Operations staff are required to complete ATS DAISEY Security Training and HIPAA training. Operations staff may also be required to complete Human Subject Research Training.

DAISEY end users receive communications that include security information, updates and tips as necessary.

Security reminders are sent to DAISEY staff every six months. This communication includes a reminder that staff are required to change their DAISEY password at least once every six months and includes updates on any relevant data governance and/or security information. The CPPR DAISEY Security Officer sends reminders to the CPPR team and the ATS Security Officer sends reminders to the operations and development teams at ATS.

6.2 Technical Safeguards

Unique User Identification
All DAISEY users have unique accounts and are prohibited from sharing usernames between multiple people. This unique account also limits users' access to data and reports available in DAISEY through Tableau Server.

Password Requirements
All DAISEY users are required to change their password every six months. All passwords are required to be at least 8 characters long with at least one upper case letter, one lower case letter, one number, and one symbol. Users are not permitted to use any of their previous 10 passwords.

Automatic Logoff
DAISEY users are automatically logged off from the system after 30 minutes of inactivity

Malicious Software
DAISEY staff guard against, and when possible, detect and report malicious software that may impact DAISEY. They guard against such software by following KU IT Security Awareness procedures for robust password management, as well as AAI policies regarding technology use. DAISEY staff are required to immediately report malicious software to the CPPR Desktop Support, and either the Lead BA (CPPR staff) or ATS Director (operations and development teams).

Log-in Monitoring

The Operations staff at ATS maintains an Access Report. This log documents incidents of attempted unauthorized access to the DAISEY system through cyber-attacks.

In addition, DAISEY logs instances of five or more consecutive failed log-in attempts. Information collected includes user information, number of total consecutive attempts, and timestamps of each attempt. After the third failed login attempt the user will receive a notification warning them that they have two more attempts before they will be locked out of their account. If there are 5 consecutive failed log in attempts, the system will lock down the user account. Users whose accounts are locked down must contact the DAISEY Admin to have their password reset.

Audit Controls
The Security Governance Board shall ensure that all of DAISEY's servers and the Tableau Server maintain appropriate audit controls.

Authenticating Information (PHI)
There is extensive access control applied to entities and individuals using the system.

Person or Entity Authentication
DAISEY staff are required to use KU issued accounts which offer extensive authentication protections through KU IT's account management systems.

For more information about KU accounts, visit

- 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

In addition, KU IT monitors server access and logs authentication failures.

Encryption
All database backups including backups stored off-site are fully encrypted using asymmetric encryption of 256 bit or greater. Encryption keys are secured and stored separately from the backups.

The DAISEY team is working to implement full back end encryption, where (1) PHI and any sensitive data is encrypted at rest on storage devices and (2) data is encrypted while transferred over the internal network between layers of the application. There are multiple layers of security controls for the DAISEY servers and other infrastructure components.

Transmission Control
The Security Governance Board shall ensure that web application traffic is encrypted during transmission using modern, secure encryption technologies.

Virtual Private Network
When working on DAISEY projects through a wireless internet connection, DAISEY staff are required to log on to KU's Virtual Private Network (VPN). This split tunnel VPN protects all traffic, whether accessing DAISEY's server or logging into DAISEY's production or fix environments on a web browser. Two relevant KU IT policies include Virtual Private Network (VPN) Service on the University of Kansas Data Network,

found at https://policy.ku.edu/IT/VPN-policy, and Virtual Private Network (VPN) Remote Access Procedure, found at https://policy.ku.edu/IT/VPN-remote-access-procedure

6.3 Data Alteration and Destruction

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. Will notify 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.

Section 7: Physical Safeguards

7.1 Physical Safeguards

Facility Access Control
Physical access to the DAISEY system is limited. The server DAISEY is held on is located in the Price Computing facility which restricts access and is monitored by staff 24/7. KU IT maintains two relevant policies, Data Center and Server Room Policy: http://policy.ku.edu/IT/data-center-server-room and Data Center and Server Room Standards at https://policy.ku.edu/IT/data-center-standards

Access Control and Validation Procedures
KU IT maintains two relevant policies, NOC Data Center Access and NOC Data Center Access for MSA Clients. This policy is not publicly available, however you may request a copy of the policy from the KU IT Security Office by submitting a form at https://technology.ku.edu/contact-it-security-office. Please reference the specific policy name listed here.

Update to - 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 or you may request a copy of the policy from the KU IT Security Office by submitting a form at https://technology.ku.edu/contact-it-security-office. Please reference the specific policy name listed here.

Maintenance Records
KU It maintains two policies relevant to records maintenance, NOC Building Security and NOC Departmental Responsibility for FSP and Facilities. This policy is not publicly available, however you may request a copy of the policy from the KU IT Security Office by submitting a form at https://technology.ku.edu/contact-it-security-office. Please reference the specific policy name listed here.

Update to - Maintenance information for the KU data center and server room can be found at https://policy.ku.edu/IT/data-center-standards#access or you may request a copy of the policy from the KU IT Security Office by submitting a form at https://technology.ku.edu/contact-it-security-office. Please reference the specific policy name listed here.

Workstation Use

CPPR DAISEY 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.

Workstation Security

All CPPR DAISEY 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.

Section 8: Security Incidents

8.1 Security Incident vs. Security Breach
A security incident occurs when an individual is able to view, access, modify or delete information that they should not have the ability to view, access, modify or delete.

A security breach is the unauthorized acquisition, access, use or disclosure of PHI that compromises security of data or privacy of client information, causing significant risk of financial, reputational or other harm to an individual. *Not all security incidents are security breaches but all security breaches are security incidents.*

8.2 Response to Security Incidents
In the event that a DAISEY staff becomes aware of a security incident, they are required to *immediately* notify the DAISEY Management Team. The Management Team will consult to determine what immediate steps to take. The Management Team will assign DAISEY staff to carry out two response requirements:

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 DAISEY staff became aware of incident
    - Data involved
    - Impacted organizations, initiatives and partners
    - Details of how DAISEY 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 will use that information to 1) determine whether there was indeed a security incident, 2) determine if the incident was a breach and 3) determine an appropriate response, such as changes to system functionality, policies and/or procedures if necessary.

8.3 Notice of Security Incident Letters
In the event that a security incident is determined to be a security breach, a Notice of Security Incident (NOSI) letter is sent to affected parties. If the security incident is not a breach, the CPPR Associate Director determines whether or not a NOSI letter will be sent to affected parties. NOSI letters contain all pertinent information gathered about the incident. CPPR sends these letters in accordance with applicable governing and contractual agreements.

8.4 Documentation of Security Incidents
The DAISEY Security Officer maintains a log that documents security incidents that occur in DAISEY. It contains information gathered about the incident, internal and external communication regarding the incident, and any response to the incident. The Security Governance Board reviews the security incident log annually in addition to reviewing the information contained within the log after each security incident.

Section 9: Evaluation and Testing

9.1 Application and Data Criticality

DAISEY staff will conduct an application and data criticality analysis once every three years. The analysis consists of the following:

- Inventory of data assets, considering the sensitivity and security required by that data.
- Assessment of data most critical in supporting the contingency plan
- Determination of which activities, materials and processes involving PHI are critical to business operations
- Estimate of an acceptable amount of time for disruption in DAISEY operations

9.2 Evaluation

The Security Governance Board arranges for or conducts a technical and non-technical evaluation of DAISEY'S compliance with all policies and procedures at least once every three years. These evaluations may be completed by a vendor of appropriate credentials and experience or by KU staff selected by the Security Governance Board.

9.3 Risk Analysis

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 once every three years. The analysis identifies risks and assets of the system as well as cost effective measures to mitigate risks.

9.4 Application and Data Criticality Assessment

A security assessment will be conducted at minimum every three years or if it is deemed necessary by ATS or the 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.

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. (See Appendix 1, Limited Data Set Identifiers)

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

Appendix C: 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 D: Version Log

December 1, 2015
Compilation of CPPR developed HIPAA Security crosswalk, KU IT provided resources, and information obtained from ATS.

January 12, 2016
Updated language in Introduction and Definitions to include FERPA.

January 9, 2019
Updated based on changes to the Charter and DAISEY Data Security Manual.