IRIS Security Policy Manual

Updated: April 2026

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 University of Kansas Center for Public Partnerships and Research (CPPR) is working to build upon existing efforts and infrastructure to ensure communities can effectively coordinate, improve, and track outcomes for children, youth, and families across the state. As part of this effort, CPPR developed Integrated Referral and Intake System (IRIS), a web-based communication and referral tool. The goal of IRIS is to support best practices in social service referral and coordination among community partners. IRIS's primary purpose is to enable service providers in a community to make, receive, track, and respond to referrals.

The IRIS Team is committed to preventing, detecting, containing, and correcting security violations in the system through creation, administration, and oversight of IRIS policies and procedures. The following Data Security policies demonstrate the ways in which IRIS complies with the Health Insurance Portability and Accountability Act (HIPAA), particularly the HIPAA Security Rule. This document describes robust administrative, technical, and physical safeguards of the IRIS system and also provides contextual information to help readers understand the structure and governing policies of IRIS.

All policies referred to in this document are either publicly available or can be made available upon request. IRIS policies and this manual may be updated twice per year.

Section 2: Security Responsibility

2.1 Structure of Responsibilities
Multiple entities have responsibilities for IRIS security. IRIS is primarily designed, administered, and supported by CPPR. CPPR manages organizations and communities within IRIS, providing support, technical assistance, and designing system infrastructure for each community. Brand New Box (BNB) provides technical development and operations of the system (e.g., programming and technical infrastructure). BNB utilizes Aptible Inc. and Amazon Web Services (AWS) for infrastructure and secure data storage. Each organization has internal data governance for regular operations that include IRIS projects.

2.2 IRIS Management Team
The IRIS Management Team is responsible for making high-level decisions regarding IRIS. Members include Deputy Director of CPPR, IRIS Security Officer, Research Project Manager, and other designees by the Deputy Director. 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 IRIS 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 IRIS as required by HIPAA.

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

2.5 AWS HIPAA Compliance
Details about Amazon Web Services HIPAA security and compliance can be found at https://aws.amazon.com/compliance/hipaa-compliance

Section 3: System Availability & Emergency Operations

In the event of an emergency (for example fire, natural disaster, system failure, or vandalism), IRIS 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 the IRIS Management Team to determine the impact the emergency had on the IRIS system. Availability of IRIS to Support Users, End Users and Developers is a secondary service that will be established only after the Operations and the IRIS Management Team have determined it is safe to do so and that IRIS will function appropriately.

3.1 Uptime
Purpose: Establish expectations for IRIS application, data, and report availability for users.

Policy Statement: The expectation is that the IRIS application and reports are generally available and accessible to users during business hours: 8 AM – 6 PM Central Time Mon-Fri. System maintenance is typically performed as necessary on Tuesdays, 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 IRIS are to be notified 24 hours in advance by CPPR staff. BNB will notify CPPR staff as far in advance as possible regarding any work that will result in an outage. All planned outages are typically conducted on Tuesdays, 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, BNB will inform the IRIS Management Team 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 BNB to restore the system to a working state as soon as possible. BNB will provide the IRIS Management 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 procedure is in place to recover the application and database within 24 hours.

3.3 Data Corruption
Purpose: Establish expectations for mitigating a data corruption situation.

Policy Statement: IRIS backups are kept for a minimum of 90 days. If data corruption is discovered within those 90 days, the IRIS Management Team can determine, with the help of BNB, to 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: Databases are stored in the AWS US-EAST-1 and US-WEST-2 regions via Aptible. Having IRIS in two regions allows for a failover between each data center in the event of a failure.

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html

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

Policy Statement: Database backups are executed nightly. Backups are stored at AWS for a minimum of 90 days. This ensures no more than 24 hours of data loss.

3.6 Emergency Server Operations
Purpose: Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

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

In the event that BNB informs the IRIS Management Team that the IRIS system has gone down, the IRIS Management Team will determine an appropriate response. This may include initiation of Emergency Mode, detailed in IRIS Security Policy 3.7.

3.7 Emergency Mode

Purpose: Protect the security of the IRIS system and all IRIS 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 IRIS Management Team may initiate the system's Emergency Mode.

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

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

Emergency Mode ends upon consensus of the IRIS Management Team and notification to BNB. Upon receipt of this notification, BNB 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 IRIS Management Team and Operations teams.

Policy Statement: An IRIS Management Team designee shall work with BNB to test Emergency Mode procedures at least once per year. The designee shall monitor and document the results of the test. The IRIS Management Team 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 community funding agencies, organizations, 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 community agency, the relationship of the community agency to its partner organizations, and status of the community agency and partnering organizations as HIPAA and/or FERPA covered entities.

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

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

IRIS Management Team Document Table

Document Name	Parties	Purpose
IRIS System Manager and Data Manager Agreement	System Managers, Data Managers and KUCR/CPPR	Establishes expectations regarding responsible and confidential management of an IRIS community by users with System Manager and/or Data Manager access.
Business Associates Agreement (BAA) (optional)	Each IRIS partner organization and KUCR/CPPR	At the request of a partner organization, the BAA shall provide written assurances that the data shared will be safeguarded appropriately.
Responsible Data Use Agreement	Each IRIS partner organization and KUCR/CPPR	The Responsible Data Use Agreement outlines CPPR's relationship to the information entered into IRIS. It also reminds organizations about responsible use of a system that contains confidential client information and the importance of discussing informed consent with clients who are the subject of a referral.
IRIS User Confidentiality and Data Security Agreement	Individual IRIS users	Establishes requirements for IRIS users to keep all IRIS information confidential and meet expected data security practices.
Community Memorandum of Agreement/Understanding (optional)	Partnering organizations within an IRIS community	Memorandum of Agreement/Understanding, otherwise known as a "cooperative agreement," is a type of legal document more formal than a verbal agreement but less formal than a contract. It sets out the *ground rules* for a collaborative relationship, including terms all partnering organizations within an IRIS community agree to how IRIS will be used and how data in IRIS will be protected.

Client Consent (optional if using existing consent forms)	Individuals who are the subject of referrals	An acknowledgement by individuals receiving services that personal information will be entered into IRIS. Organizations may use already existing forms.

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 organization violates the terms of a data governance document to which they are a party, the IRIS Management Team shall work with community representatives to conduct a formal 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 organization's access to IRIS.

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 IRIS Security Policy 8.4.

Section 5: User Access

5.1. Access Control
Purpose: Ensure that all users have appropriate access to IRIS and to prevent those who are not authorized to have access from obtaining access.

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

5.2 Systems Groups
Purpose: Restrict access to data for individuals having approved contact with IRIS.

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

System Group	Description	Data Access
Development Team	BNB Team that develops the technical specifications of the system.	Access to live identifiable data in application and database
IRIS 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. This group is limited to only a few staff because of the high-risk level associated with its access.	All data in application
End Users	Individuals using the system for its intended purpose as a communication and referral 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 IRIS to only the parts of the system necessary to perform their job duties.

Policy Statement: Access for individuals in contact with IRIS 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 IRIS as described below:

System Environment	Access by Group	Data Type	Purpose
Production	Development Team, IRIS Management Team, Support Users, and End Users	Contains real, live, identifiable data	Administration by IRIS Management Team and Support Users. End Users enter and submit real data.
Training	Development Team, IRIS Management Team, Support Users (as needed), and End Users (as needed)	Contains fake data for training purposes	Used for training new users with the IRIS application.
Staging	Development Team, IRIS Management Team, and Support Users (as needed)	Contains fake data	Final testing by the IRIS Management Team and development teams. Support users may provide testing support to IRIS Management Team.
Local	Development Team	Contains fake data	Initiate development changes in IRIS.

5.4 User Roles

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

Policy Statement: IRIS 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. Users may be assigned "switch access" between multiple IRIS Organizations/Communities if deemed appropriate for their job duties.

The following user roles are available in IRIS:

- User – unrestricted access to data within organization
- Implementation User – unrestricted access to community implementation documentation within their community
- Data Manager – unrestricted access to data within their community (across organizations)
- System Manager can add/edit/remove organization information, add/edit/remove users, edit community configuration

- System Admin – unrestricted access to data within IRIS, ability to add/edit/remove configurations

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

Policy Statement: Access rights for development are fixed. Fixed is defined as having root access to all data. Access rights for CPPR staff are flexible. The IRIS Management Team, and ultimately a designee from the IRIS Management Team, is responsible for ensuring that CPPR staff have the appropriate role and minimum level of access required to complete job duties.

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

• Do they require access to the staging environment?
• Do they require access to real data or just the training module?
• Do they require access to a single community or multiple communities?
• Do they require administrative privileges for one or more communities?
• Do they need System Manager and/or Data manager privileges for one or more communities?

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

5.6. Access Establishment

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

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

Initial access and access edits for the Development Team must be approved by the IRIS Management Team in Local, Staging, Training, and Production environments. Access edits for the Development Team in the Local, Development, Staging, and Production environments may be made by the Development Team.

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

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

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, IRIS Management Team, and System Managers. Primary IRIS Contacts verify any IRIS access requests before access is

granted or modified. Access shall be granted to an End Users only after the user agrees to the terms of the User Confidentiality and Data Security Agreement (Appendix D) by clicking "Agree" upon their initial login and annually thereafter.

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 IRIS 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 IRIS End User access is regularly reviewed, monitored, and edited as necessary.

Policy Statement: System Managers shall modify End User access upon request from the user's organization point of contact. CPPR staff can act as a System Manager for some IRIS communities. System Managers will conduct yearly audits of user access. Users will be automatically deactivated by the IRIS system after four months of inactivity.

5.7 Documentation of User Access

5.7.1 Review of CPPR Staff Access
Purpose: Track CPPR staff access permissions in IRIS to accurately document current staff roles in the system and maintain a history of staff access and roles.

Policy Statement: IRIS maintains a record of all active and inactive accounts. The IRIS Management Team (or designee) shall review and update CPPR staff access in IRIS at least quarterly. This review shall consist of confirming that CPPR staff still need access to all communities, organizations, and roles for which they have active accounts in IRIS. The IRIS Management Team (or 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 BNB.

5.8 Sanction Policy

5.8.1 CPPR Staff Inappropriate Usage Sanctions
Purpose: Outline potential sanctions that would constitute an appropriate response to CPPR staff inappropriate use of IRIS or inappropriate access to data.

Policy Statement: As described by the University of Kansas's General Acceptable Use of Electronic Information Resources:

Acceptable Use of Electronic Information Resources | Policy Library (ku.edu)https://policy.ku.edu/IT/AcceptableUse

Remote Work Policy Remote Work Policy | Policy Library (ku.edu)

Data Classification and Handling Policy Data Classification and Handling Policy | Policy Library (ku.edu)

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 IRIS policy regarding IRIS, the Director of CPPR or designee will determine appropriate response to misuse, abuse or fraud involving IRIS. All pertinent KU Human Resource policies and procedures will be followed.

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

Policy Statement: CPPR may terminate the IRIS account of any End User who is found to have violated the IRIS Confidentiality and Data Security Agreement.

If an End User is suspected of having violated the IRIS Confidentiality and Data Security Agreement or inappropriately access data or abused their access to IRIS in any way, the IRIS Management Team will work with community 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 KU IT Security Awareness Training, and Human Subject Research Training prior to being granted access to the system and at least every three years.

Note: Policies describing required trainings for non-CPPR IRIS staff are maintained by BNB.

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 CPPR 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 IRIS 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: The IRIS Support Users shall send periodic e-mails to IRIS 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 IRIS system and data access to only approved individuals and ensure that user actions within the system are linked to individual users.

Policy Statement: Each IRIS user will have a unique username and password. End Users must agree that sharing their login information is prohibited during the first time of account log in.

6.2.2 Password Requirements

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

Policy Statement: The IRIS system requires a minimum of 8 characters, at least 1 uppercase letter, 1 lowercase letter, 1 number, and 1 symbol. Passwords cannot match any of the last 10 passwords used.

6.2.3 Multifactor Authentication

Purpose: Promote system security by requiring users to enter a TOTP (time-based, one-time password) during the login process.

Policy Statement: The IRIS system requires the user to enter the time-based, one-time password once each calendar week when logging in. This one-time password is provided to the user from an authenticator application of their choice. Some examples of authenticator apps include Google Authenticator, Microsoft Authenticator, and Duo. This ensures that the person accessing the account must use multiple devices to prove their identity and to avoid unauthorized access to sensitive data. In addition to using authenticator applications for MFA (multifactor authentication), IRIS also supports hardware keys, such as key fobs, that may be used as an alternative to using an authenticator app on the user's device.

6.2.4 Automatic Logoff

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

Policy Statement: A user's session will be automatically logged off after 30 minutes on inactivity.

6.2.5 Malicious Software

Purpose: Protect the IRIS 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, the IRIS Management Team, and BNB.

6.2.6 Login Monitoring

Purpose: Protect the integrity of the IRIS system by monitoring unauthorized access attempts and failed login attempts.

Policy Statement: User accounts will be locked after five failed log in attempts. The user will see a message after three failed attempts to alert them that their account is about to be locked. The messaging will provide helpful links to prompt the user to change their password if needed before their account is locked. After their fifth failed login attempt, they will receive an alert that their account is now locked and that they must contact the IRIS help desk to have their account unlocked.

6.2.7 Audit Controls

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

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

6.2.8 Person or Entity Authentication

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

Policy Statement: IRIS authenticates users based on unique usernames and passwords. IRIS also uses multifactor authentication to authenticate a user during the login process. Users must download and install an authenticator application on an external device and use the TOTP (time-based, one-time password) that is provided by the authenticator to log in and verify their access.

6.2.9 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.

6.2.10 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: BNB shall ensure that data is encrypted via SSH or HTTPS during transmission.

Confirmation of encryption should be included in the Risk Analysis (see IRIS Security Policy 9.1) and Application and Data Criticality Analysis (see IRIS Security Policy 9.3).

6.3 Data Alteration and Destruction

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

Policy Statement: The IRIS Management Team can determine that due to technical requirements of the IRIS application or database, data may need to be altered or destroyed outside of the application. If determined, the IRIS Management Team will develop a plan with BNB 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 BNB to ensure recovery in case it's needed. The special backup will expire and/or be deleted within 90 days.

AWS Overview of Security Processes

https://aws.amazon.com/whitepapers/overview-of-security-processes

Elastic Block Storage (Amazon EBS) Security

As of 8/19/2019 "… Amazon EBS volumes are presented to you as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse so that you can be assured that the wipe process completed. If you have procedures requiring that all data be wiped via a specific method, such as those detailed in NIST 800-88 ("Guidelines for Media Sanitization"), you have the ability to do so on Amazon EBS. You should conduct a specialized wipe procedure prior to deleting the volume for compliance with your established requirements. …"

Data Sanitization

As of 8/19/2019 "Data Sanitization Amazon EFS is designed so that when you delete data from a file system, that data will never be served again. If your procedures require that all data be wiped via a specific method, such as those detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization"), we recommend that you

conduct a specialized wipe procedure prior to deleting the file system.”

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:
Amazon AWS controls physical access. See policies here: https://aws.amazon.com/compliance/data-center/controls

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: Amazon AWS controls physical access. See policies here: https://aws.amazon.com/compliance/data-center/controls

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

Policy Statement: Amazon AWS controls physical access. See policies here: https://aws.amazon.com/compliance/data-center/controls

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.

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 IRIS 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 IRIS 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 become aware of a potential security incident shall *immediately* notify the IRIS Management Team or designee via e-mail. The members of the IRIS 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
    - Type of data involved
    - Impacted organizations, communities, 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 IRIS 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 IRIS Management Team shall ensure that Notice of Security Incident Letters are sent in accordance with policy CPPR IRIS Security Policy 8.3.

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 IRIS Management Team determines to be a security breach, they shall send a Notice of Security Incident (NOSI) letter to all affected parties. If the security incident is not a breach, the CPPR 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: The IRIS Management Team or designee shall maintain a log documenting IRIS 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 IRIS Management Team shall review the security incident log annually in addition to reviewing incident-specific information within the log after each security incident. The IRIS Management Team 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 IRIS Management Team or designee 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 IRIS system.

Policy Statement: The IRIS Management Team or designee conducts or arranges for an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of information in the IRIS system. A security audit will be conducted at a minimum every three years or if it is deemed necessary by BNB or the IRIS Management Team due to significant changes to the software application. The assessments will be logged in the IRIS 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 sufficiently to reduce risk and vulnerabilities to an appropriate level.

Policy Statement: The IRIS Management Team reviews 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 IRIS Management Team. Audit activities will occur every three years and audit check-ins will occur as needed.

Appendix A: Definitions

Client Consent - Client consent means that an individual or family has agreed to allow limited personal information to be entered into IRIS as part of a referral for services. Users are required to acknowledge that they have obtained client consent each time they create a Family Profile and each time they make a referral in IRIS. Organizations recognize their own requirements to externally receive client consent. Organizations may use or modify the client consent template provided by IRIS, or work from an existing client consent document within their Organization.

Community - A community is a network of organizations that use IRIS to refer the individuals and families they serve to partner organizations within the same community, geographic region, or service area.

Community Champion - The Community Champion is the person selected to lead the IRIS implementation process for their community. This includes acting as the liaison between community members and the IRIS Implementation Team and facilitating community-wide discussions. A Community Champion is also a data champion, utilizing IRIS data to make sure the network has the greatest possible impact for local individuals and families.

Community Standards - Community Standards are shared expectations developed and agreed upon by partner organizations in the IRIS community. This includes the community's vision, use of IRIS for referrals, workflow requirements, and training. Once finalized, the Community Standards are housed in the Community Documents section of IRIS for all users to access.

Data Manager- The Data Manager has access to all referral data for their community, including Family Profile data, allowing them to compile aggregate community level data for discussion by IRIS partner organizations, and handles all data-related inquiries. In some cases, the same person will fill the Community Champion, Data Manager, and System Manager roles.

Family Profile - The Family Profile holds contact information for the adult consenting to the referral, either for themselves or their children. The profile records the least amount of information necessary to make a referral: the adult's first name, last name, date of birth (to avoid duplicate profiles), phone number and/or e-mail. Specific referral information, including information about children referred for services (if applicable), is contained in the Referral Information Fields, accessed after a specific referral organization has been selected for the individual or family.

Memorandum of Agreement/Memorandum of Understanding - The Community Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU), otherwise known as a "cooperative agreement," is a legal document more formal than a verbal agreement, but less formal than a contract. It sets out the ground rules for a collaborative relationship. The MOA/MOU establishes terms agreed on by all partner organizations within an IRIS community regarding IRIS use and data protection. The community determines if this type of agreement is needed.

Organization - An Organization is a referral partner in the IRIS community. Partner organizations with distinct programs that include different staff, services, and eligibility requirements often choose to set up each program as a separate "Organization" in IRIS.

Organization Details - Each organization in IRIS is responsible for providing details about their organization on the My Organization screen. This information is available to partner organizations in the IRIS community and includes contact information, the type of services provided, and any eligibility criteria. Organizations are encouraged to keep this information updated to ensure accurate referrals.

Primary IRIS Contact - The Primary IRIS Contact name and phone number for each organization appears on the organization's profile. This information is accessible to all users via the Partner Organizations screen and the See Details section of each referral card. The Primary IRIS Contact at each organization should be a person who can answer questions about services offered, eligibility, and the use of IRIS within the organization.

Referral Information Fields - Referral Information Fields contain details about the referred individual or family that are shared when a referral is made in IRIS. These fields are customized by each IRIS community.

Responsible Data Use Agreement - The Responsible Data Use Agreement outlines CPPR's relationship to the information entered into IRIS. It also reminds organizations about responsible use of a system that contains confidential client information and the importance of discussing consent with clients. The Responsible Data Use Agreement must be electronically signed before an organization is granted access to IRIS.

Responsible Data Use Contact - Each organization must identify a Responsible Data Use Contact who will receive an e-mail with a link to electronically agree to the IRIS Responsible Data Use Agreement. The Responsible Data Use Contact should be someone with the authority to accept these terms on behalf of the organization.

Sectors/Sector Tagging - Sectors represent the categories within which an organization operates. Users can select up to two sectors on the Organization Information page: a Primary Sector and a Secondary Sector. The Primary Sector is required and should be selected based on the organization's core services. The Secondary Sector is optional and includes "Other," allowing users to provide a custom response. The sector affiliations chosen are reflected in the Sector Report, which provides an overview of a Community's sector representation.

Service Areas - Service Areas are filters that allow IRIS users to search for referral partners based on the services they provide. These fields are customized by the IRIS community. When making a referral, users may choose one or more Service Areas to narrow the list of potential referral partners.
Organizations should keep their Service Areas updated to ensure the accuracy of referrals.

System Manager - The System Manager handles technical activities, including serving as the IRIS administrator, and primary contact person for application. In some cases, the same person will fill the Community Champion, Data Manager, and System Manager roles.

Team Member - A Team Member is a user at a partner organization in an IRIS community.

Terms of Use - Some funders require a Terms of Use document to establish guidelines for data collection and IRIS use. This document outlines what data will be entered into IRIS, how it will be used, and how it will be protected. The funder determines if this type of agreement is needed.

User Access - There are three levels of user access in IRIS: basic, System Manager and Data Manager. Team Members with basic user access can make and receive referrals in IRIS, and view all referrals and data involving their organization. Data Managers have the added ability to see referral data for the community at large, including Family Profile data. In addition to their administrative capabilities, System Managers have data access limited to Community Wide Capacity data.

User Confidentiality and Data Security Agreement - All users must agree to the User Confidentiality and Data Security Agreement the first time they log into IRIS. This agreement sets out requirements for users to keep all IRIS information confidential and meet expected data security practices.

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 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.

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).

Appendix B: IRIS User Access Audit Logs

The IRIS User Log can be exported from IRIS as a downloadable CSV.

IRIS User Log Example

First Name	Last Name	Phone	Email	Communit	Organizati	Implemen	Receives n	Receives r
First Name	Last Name	555-555-5	firstname1	Care Com	Referral Partner,Hom		Yes	Yes
First Name	Last Name	555-555-5	firstname2	Friends Co	Health Department		Yes	Yes
First Name	Last Name	555-555-5	firstname3@veryrealemail.com			Care Com	No	No
First Name	Last Name	555-555-5	firstname4@veryrealemail.com			Care Com	Yes	Yes
First Name	Last Name	555-555-5	firstname5@veryrealemail.com			Friends Co	No	No
First Name	Last Name	555-555-5	firstname6	Friends Co	Centralized Intake		Yes	Yes
First Name	Last Name	555-555-5	firstname7@veryrealemail.com			Healthy Fa	No	No
First Name	Last Name	555-555-5	firstname8@veryrealemail.com			Healthy Fa	No	Yes
First Name	Last Name	555-555-5	firstname9	Friends Co	Health Department		Yes	Yes

Note: This example is a Worksheet Object. You will need to open it to view the example in its entirety.

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: IRIS User Confidentiality and Data Security Agreement

IRIS User Confidentiality & Data Security Agreement

University of Kansas Center for Public Partnerships & Research
IRISadmin@ku.edu

Your organization has agreed to partner with the University of Kansas Center for Public Partnerships and Research to provide access to Integrated Referral and Intake System (IRIS), a web-based communication application.

This Agreement must be read and agreed upon by each IRIS User before an account is activated. Violation of this Agreement is grounds for termination of an individual's IRIS account.

Data

IRIS input consists of limited personally identifiable demographic information on children, families, and households; information contained in measurement and assessment instruments; and aggregate information from organizational reports (herein referred to as "Data").

Data entered into IRIS belongs to your organization, partnering organization, and any funding agencies providing access to IRIS for your community.

Confidentiality

All data held within IRIS shall be treated as confidential. The confidentiality of the data and the trust and confidence placed in you by your clients and partnering agencies must be protected at all times.

In particular, IRIS users agree to:

1. Comply with all relevant Terms of Use Agreement, Community Memorandum of Agreement, and Contract Agreements your organization has established.

2. Not share login information with anyone.

3. Report loss of a password, any actual or attempted unauthorized access, use, or disclosure of PII/PHI to IRIS Admin (irisadmin@ku.edu) immediately.

4. Use and access IRIS solely for the purpose of sending, receiving, and updating information on referrals.

5. Follow all federal, state, and local laws and regulations applicable to your collection, sharing, and distribution of the Data.

University of Kansas Center for Public Partnerships & Research
IRISadmin@ku.edu

Appendix E: IRIS Responsible Data Use Agreement

IRIS Responsible Data Use Agreement

Your organization agrees to use the **IRIS referral platform** to coordinate referrals for services with other partner organizations who serve families in your community. That means that your organization will help families understand what IRIS is, how it works, and **always give families the choice to consent** for their personally identifying information (PII) (e.g., contact information, demographics, needs) to be shared with other partner organizations who serve families in your community. Users in your organization will adhere to responsible use of IRIS and treat a family's information as confidential. Users in your organization may not use any of the PII in IRIS for any other purpose than to coordinate referrals for services. Your organization certifies that all users have been trained on how to use IRIS, understand responsible use of the information shared among partners, and understand your organization's consent process prior to using IRIS. If consent and responsible use procedures are not followed, your organization's access to IRIS may be removed. The University of Kansas shall not be held liable for any actions stemming from misuse of IRIS or non-authorized disclosure of information contained within it by your organization.

The IRIS referral platform and the information contained in it are hosted on a HIPAA-compliant server to keep PII secure and safe. IRIS is not designed nor intended to host, transfer, or collect personal health information (PHI) about a family. Information in IRIS belongs to the families who provide consent, your organization, partnering organizations in the community who are part of a referral, and any funding agencies supporting access to IRIS for your community. The University of Kansas Center for Public Partnerships and Research (KU-CPPR), who developed and maintain the IRIS platform, may access information in IRIS to provide technical assistance to IRIS users, to support continuous quality improvement in your community, and to evaluate IRIS for impact. KU-CPPR will only report or present de-identified, aggregate family data for such activities.

You, acting on behalf of your organization, hereby agree to hold harmless, defend and indemnify University of Kansas and its officers, directors, employees, agents, affiliates, successors, and assigns from any and all claims, actions, or losses for bodily injury, property damage, wrongful death, emotional distress, or other damages or harms (collectively, "Claims"), whether to your organization or to third parties, which may result from your organization's use of the IRIS application; provided however, in no event shall your organization be liable for any claims resulting from the negligent or wrongful acts or omissions by KU-CPPR or its employees.

You, acting on behalf of your organization, acknowledge and agree that the IRIS application and all intellectual property rights associated therewith are, and shall remain, the property of Licensor. The IRIS system may utilize or include third party software that is subject to third party license terms ("Third Party Software"). You, on behalf of your organization, acknowledge and agree that your organization's right to use such Third Party Software as part of the IRIS system is subject to and governed by the **terms and conditions of the third party license** applicable to

such Third-Party Software. In the event of a conflict between these Terms and the terms of such third-party license(s), the terms of the third-party license(s) shall control with regard to your organization's use of the relevant Third-Party Software.

Licensor, on behalf of itself and its affiliates, third party service providers, licensors, and suppliers, hereby disclaims all warranties. The IRIS system and services are provided "As-Is" and "As Available." To the maximum extent permitted by law, Licensor, on behalf of its affiliates, third party service providers, licensors and suppliers, expressly disclaims any and all warranties, express or implied, regarding the IRIS application and services, including, but not limited to, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement of intellectual property or other violation of rights. Licensor, on behalf of itself and its affiliates, third party service providers, licensors and suppliers do not warrant that the IRIS system or the services will meet your requirements, or that the operation of the IRIS system or the services will be uninterrupted or error-free. Further, no warranty nor representation is made concerning the accuracy, likely results, or reliability of the use of the IRIS application or services.