Data Governance and Client Confidentiality

Since conversations about data privacy often arise as part of the IRIS Organization onboarding process and affect how your partners will interact with the system, data governance requirements should be considered early in the IRIS implementation process.

IRIS DATA GOVERNANCE

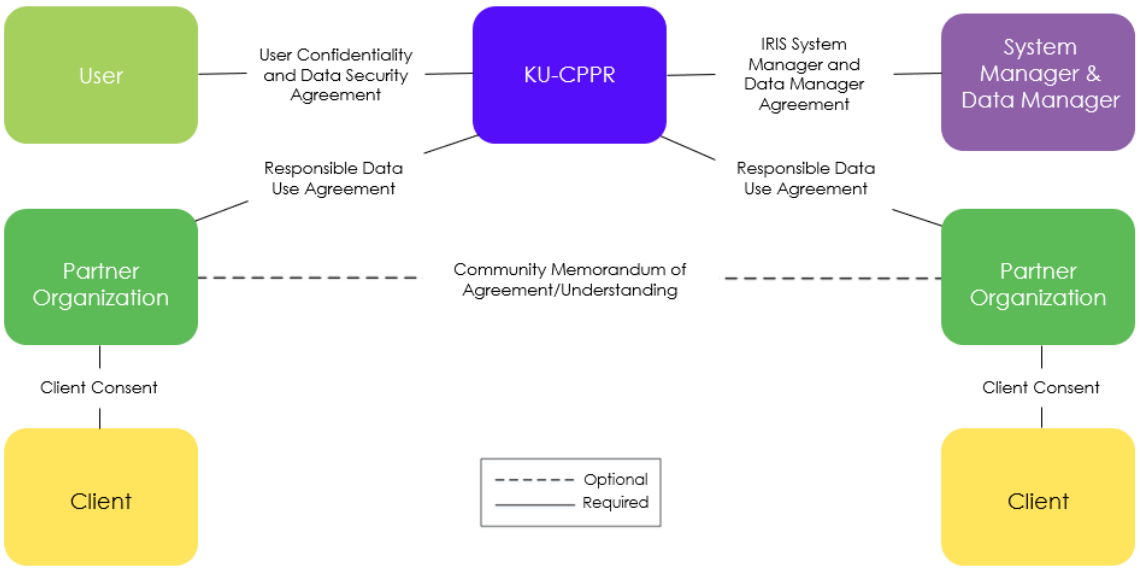
IRIS seeks to maintain the privacy and security of personal information, including compliance with administrative, technical, and physical controls to safeguard personal information from unauthorized access, use, or disclosure.

The diagram below provides examples of data agreement relationships in IRIS. A detailed description of each document follows in the next section.

As you review, we encourage you to:

- Note what is required and plan for integrating that into your existing referral workflows.
- Consider if any optional agreements (e.g., will a Memorandum of Agreement (MOU) or Business Associate Agreement (BAA) be needed? How can you work with your partners to ensure these are addressed?

Consider if any additional data governance agreements, such as those outlined in the last section, may be needed in your community.



IRIS DATA AGREEMENTS – SUMMARY

Client Consent

Client consent is acknowledged prior to any referral being sent through IRIS and is an acknowledgement by individuals receiving services that their personal information will be entered into the system.

Parties: Individuals who are the subject of referrals and IRIS users making the referral on their behalf.

Modification: Organizations may either adopt the practices outlined in the **Client Consent Template**, modify the template, or modify an existing client consent process.

Required/Optional: Required. While organizations or a community may use their own client consent forms, they must confirm that family consent was obtained before creating a referral.

Community Memorandum of Agreement/Understanding (MOU)

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 IRIS Organizations agree to regarding how IRIS will be used and how data in IRIS will be protected.

Parties: Organizations within an IRIS community.

Modification: This document may be modified as necessary by participating organizations.

Required/Optional: Optional. The community may already have an agreement in place or determine an additional agreement is not necessary.

IRIS Manager Agreement

Establishes expectations regarding responsible and confidential management of an IRIS community by users with System Manager and Data Manager access.

Parties: System Managers and Data Managers.

Modification: This document shall be modified only by KU-CPPR.

Required/Optional: Required. System or Data Manager access will not be given until an individual receives appropriate training and signs the Manager Agreement.

Responsible Data Use Agreement

The Responsible Data Use Agreement outlines KU-CPPR's relationship to the information entered into IRIS. It also reminds IRIS Organizations about the 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.

Parties: Each IRIS Partner Organization.

Modification: This agreement shall be modified only by KU-CPPR.

Required/Optional: Required. IRIS Partner Organizations will not gain system access until the Responsible Data Use Agreement is signed.

User Confidentiality and Data Security Agreement

Establishes requirements for IRIS users to keep all IRIS information confidential and meet expected data security practices.

Parties: Individual IRIS users.

Modification: This document shall be modified only by KU-CPPR.

Required/Optional: Required. IRIS users must agree to the terms of the agreement before gaining access to the system.

IRIS GUIDANCE FOR FEDERAL DATA GOVERNANCE POLICIES

In some cases, organizations will also be required to follow federal data governance policies. While IRIS directly addresses some of these (e.g., HIPPA), organizations may need to consider adaptive guidance to ensure they are aligning their IRIS usage with the expectations of these regulations.

Organizations are responsible for considering whether any additional data governance agreements or practices may be needed in your community.

42 CFR Part 2 Regulation

Some organizations that handle substance use data are subject to the policies outlined in the 42 CR Part 2 federal regulation which concerns the disclosure of information that "would identify a patient as an alcohol or drug abuser…" (42 CFR §2.12(a) (1)). The data protected by this regulation is any information disclosed by a covered program that identifies an individual directly or indirectly as having a current or past drug or alcohol problem or as a participant in a covered program.

Partner Organizations that handle substance use data should consider best practices when using IRIS. However, it is the responsibility of all IRIS Organizations to develop referral policies and procedures that align with applicable data-sharing rules and regulations.

Further guidance on integrating 42 CFR Part 2 policies into your Partner Organization's workflows can be found in **42 CFR Part 2 Regulation: Guidance for IRIS Organizations**.

HIPAA

IRIS and its supporting data storage solution meet the data transmission and storage requirements included in the technical regulations of the HIPAA security rule. KU-CPPR and third-party vendors have policies and procedures, as well as appropriate Business Associate Agreements in place to ensure compliance with the administrative regulations of the HIPAA Security Rule.

Further guidance on HIPAA policies can be found in the **HIPAA Data Privacy and Considerations for IRIS Organizations**.

SOPPA

Some school-based organizations in Illinois may be subject to the requirements of the Student Online Personal Protection Act (SOPPA), which regulates how student data is collected and shared by educational technology providers (105 ILCS 85). Under SOPPA, an "operator" is defined as a provider of an online service or application that is both designed and marketed for K–12 school purposes and used primarily for those purposes.

IRIS was not designed or marketed as an educational technology tool and, in most IRIS Communities, is not used primarily for K–12 purposes. Therefore, IRIS generally does not meet the definition of an "operator" under SOPPA. However, individual school districts and IRIS Communities should assess their specific use of IRIS to determine applicability.