PRIVACY & SECURITY REVIEW FRAMEWORK

The Privacy & Security Review Framework is designed to help communities evaluate and strengthen their internal policies and procedures related to HMIS data protection. Like the other tools in this series, this framework supports a proactive, structured approach to privacy and security—ensuring your practices not only align with federal expectations but also reflect your community's values around data stewardship.

This tool can help your team:

- Assess whether existing policies are complete, up-to-date, and in compliance with all funder and regulatory requirements, including those outlined by HUD requirements, HIPAA, and 42 CFR Part 2
- Identify gaps or inconsistencies across core domains like consent, access, incident response, and legal oversight
- Document risks and prioritize areas for policy development or revision
- Align internal practices with HUD's privacy and security guidance and broader community goals

By reviewing policies through both a practical and compliance lens, communities can build stronger foundations for secure, ethical data use—and improve their readiness for audits, data sharing decisions, and governance conversations.

Recommended Use:

- Conduct reviews at least annually or when significant changes occur (e.g., staffing transitions, new data-sharing partnerships, regulatory shifts)
- Engage a cross-functional team for evaluation, including your CoC lead, HMIS lead agency, legal counsel, and governance stakeholders
- Pair this tool with the Data Inventory Guide and Interoperability Evaluation Matrix for a comprehensive review of your HMIS privacy and security practices

Domain	Review	Strong Policy Indicators
Data Collection & Minimization	• Do we have a current data inventory with all data elements in use throughout CoC? • Are we only collecting what's necessary? • Are optional fields clearly labeled?	• Fields reviewed for necessity annually • Optional fields limited • Includes all HUD-required data elements • Programs handling substance use follow 42 CFR Part 2
Consent & Client Notification	• Is client consent informed and documented? • Do we provide plain-language notices? • Do we have a clear process for records handling when a client does not consent to sharing PII? • Do we have a clear process for revocation of consent?	•Consent forms reviewed annually • Clear language, translated • Includes HUD consent language and 42 CFR Part 2 disclosures if applicable. • Includes language and process for specific sub-populations such as clients eligible for HOPWA, fleeing domestic violence, and unaccompanied minors
User Access & Authentication	• Are user roles clearly defined? • Are offboarding and deactivation processes closely enforced? • Is MFA required?	• Role-based access enforced •Offboarding within 24hrs • MFA active • Access policies align with HUD TA guidance
Data Sharing & Interoperability	• Are all data sharing arrangements documented? •Do we review them regularly?	• MOUs & annual review cycle in place • Transparency statements posted • Data sharing agreements align with local and federal compliance requirements
Incident Response & Breach Notification	• Do we have a clear breach response policy? • Is there a communication protocol?	• Written plan exists • Roles assigned & communicated • Simulated drills conducted • Response protocols align with state/federal breach notification laws.
Training & Capacity Building	•Do staff understand their data responsibilities? •Is training ongoing and role-specific?	• Annual and onboarding training • Security/privacy attestations and checklists submitted by participating agencies at least bi-annually • Role-based training & refreshers • Includes HUD privacy training and documentation
Governance & Oversight	•Are privacy/security standing topics at governance meetings? •Are audits conducted?	• Governance body reviews logs/reports quarterly • Compliance issues reviewed and documented regularly
Legal Compliance & Review	•Have policies been reviewed by legal counsel? • Do we comply with HUD and local laws?	• Reviewed in past year • Legal review included in changes • Ensures compliance with all applicable state/federal laws