Legal and Policy Foundations of HMIS Data Privacy & Security

Bitfocus

This document outlines key federal laws, regulations, and policies that govern the privacy and security of data collected and maintained in Homeless Management Information Systems (HMIS). It is designed for Continuum of Care (CoC) leads, HMIS administrators, direct service staff, and policymakers who are familiar with homeless response systems but may not be experts in data privacy and protection. The goal is to help communities understand the legal foundations of HMIS data protections, the obligations they impose, and the consequences of non-compliance to support policy development, risk management, and informed decision-making.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
HEARTH Act (2009)	A federal law that requires every CoC to implement an HMIS and directs HUD to establish national privacy and security protections, including: • Encryption of HMIS data • Documentation of data use/disclosure • Access controls • Client privacy rights It emphasizes safeguarding of personal data and contemplates criminal and civil penalties for unlawful disclosures, ensuring strong privacy foundations for HMIS data.	Client-level information on individuals and families experiencing homelessness that is collected and maintained in HMIS for CoCs and HUD-funded programs. HMIS must uphold privacy protections for this information while performing its required tasks.	All HUD-funded homelessness programs, including both recipients and subrecipients of CoC and ESG funding, are required to participate in HMIS and comply with all relevant provisions of the HEARTH Act.	Non-compliance can jeopardize HUD funding and CoCs that fail to implement HMIS or protect collected data could lose grant awards or face monitoring findings. The HEARTH Act also incorporates legal penalties for unauthorized HMIS disclosures. Agencies and agency staff may be individually responsible for improper disclosure of sensitive client data.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
HUD HMIS Data & Technical Standards	HUD's baseline standards for HMIS privacy and security. These standards "seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data." Key protections include: • Requiring a posted privacy notice (so clients understand their rights) • Obtaining consent when needed for data sharing, through a signed Release of Information (ROI) • Limiting data collection to what is necessary • Implementing security measures such as password, user access levels, encryption, training, etc. • Upholding client rights (e.g., right to access their data, object to certain sharing, etc.)	All Protected Personal Information (PPI) about clients in HMIS (i.e., any information that can be used to identify a specific person). This includes: • Name • Social Security Number • Date of Birth • Related Service Information • Etc. The standards govern how HMIS data is collected, stored, used, and shared. While they set a national privacy floor, local implementations can add more strict state or local confidentiality rules.	CoCs and any Covered Homeless Organizations (CHOs) that collect or manage HMIS data. All HMIS participating agencies (e.g., shelters, housing programs, HMIS Leads, etc.) are bound by HMIS privacy and security rules.	Enforced via HUD and CoC oversight of CoCs and recipients/ subrecipients. Failure to adhere to HMIS standards can lead to • Findings • Corrective actions • Loss of funding Data breaches can trigger other consequences, such as: • Notification requirements • Fines • Loss of client trust in HMIS As such, non-compliance can expose agencies to HUD sanctions, liability for data incidents, and reputational damage.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
Violence Against Women Act (VAWA)	A federal law that imposes strict confidentiality requirements that override HMIS data-sharing for victim service providers (VSPs). It forbids the sharing or entry of any personally identifying information (PII) about survivors of domestic violence, sexual assault, stalking, or human trafficking into a shared database like HMIS without the survivor's informed, written consent. This protection is designed to keep survivors' locations and identities confidential. VSPs are exempt from standard HMIS data requirements and instead use a separate "comparable database" that meets HUD's technical standards to maintain strict client safety and anonymity, such as disclosing their location or identity could endanger them.	All PII about survivors of domestic or sexual violence, including anything that could identify a survivor such as: • Name • Contact information • Birth date • Social Security Number • Demographic details • Case details • Etc. Such data may not be disclosed through HMIS and only non-identifiable, aggregate data (e.g., total number of persons served, demographic counts that don't identify individuals, etc.) may be provided for the purpose of HUD reporting. If a client provides consent to share data, such consent must be "written, informed, and reasonably time-limited," usually not lasting for more than 30 days.	VSPs that serve survivors of domestic violence, sexual assault, stalking, or human trafficking and are funded by federal homeless assistance (e.g., CoC or ESG) programs or other federal affordable housing programs, in addition to other funding sources. All VSP staff/ volunteers are also bound by VAWA confidentiality requirements.	Strictly enforced, and violations can lead to loss of funding or other sanctions. HUD specifically forbids CoCs from penalizing VSPs for withholding PII from HMIS. The risks of a breach are immediate and grave: unauthorized disclosure could endanger the client's life and safety. Staff can face termination, and the agency could face legal liability and reputational damage.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
24 CFR Part 2 ("Part 2")	A set of federal regulations protecting substance use disorder (SUD) treatment records. These rules strictly prohibit disclosure of any information that would identify someone as having applied for or received SUD treatment in a federally assisted program unless the patient provides written consent. This is more restrictive than general medical privacy rules to encourage people to seek treatment without fear of exposure. In the HMIS context, this means that details of a client's substance abuse treatment cannot be entered or shared in HMIS with identifying information unless consented to each time.	All patient records about SUD diagnosis, referral, or treatment from Part 2 programs, such as: • Enrollment • Attendance • Progress • Any information that reveals they have a substance use issue In the HMIS context, this means that fields or case notes that would identify someone as a substance use treatment patient are subject to Part 2 and should be excluded or entered in a very limited way (with consent or anonymized).	Federally assisted alcohol and drug treatment programs, such as: • Clinics • Detox programs • Rehab services that receive federal funding (e.g., SAMHSA grants, Medicaid, etc.) Any CHO that qualifies as a Part 2 program or has a Part 2 division is bound by these rules. Other HMIS-participating agencies might encounter Part 2 when referring patients to treatment and should be careful not to record or disclose SUD treatment information without consent.	Serious legal consequences for violation, including civil fines of up to $1.5 million for serious breaches, federal investigation, and other sanctions. Violations undermine trust and could deter people from seeking help. Staff could face termination, and agencies may lose licenses or federal funding if they violate these requirements.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
Health Insurance Portability & Accountability Act (HIPAA)	The primary Federal health privacy law governing how personal health information (PHI) is handled. Health care providers, health plans, and related entities must safeguard individuals' medical information and can only use or disclose it for certain allowed purposes (treatment, billing, etc.) or with patient consent. In the HMIS context, any CHO that is a healthcare provider or "covered entity" must treat relevant client data as PHI and protect it (e.g., not share diagnoses or health details in HMIS without consent or de-identification).	PHI includes any individually identifiable health information such as: • Physical or mental health conditions • Treatment provided • Payment for healthcare In the HMIS context, covered agencies may not share several categories of information without proper consent, including: • Health diagnoses • Disability status • Mental health or substance use history • Medications • Treatment records	Covered entities include healthcare providers (e.g., hospitals, clinics, Health Care for the Homeless programs, mental health centers) and their business associates. In the HMIS context, this means any CHO that is providing health services and billing insurance is likely bound by HIPAA for any PHI they manage. They may require the HMIS Lead to sign a Business Associate Agreement if it handles PHI on behalf of a covered partner because the HMIS Lead would be handling PHI on behalf of the healthcare provider.	Enforced by the US Department of Health and Human Services and can result in civil fines of $100 to $50,000 per violation, capped at $1.5 million per year for each type of violation. In extreme cases, breaches can lead to criminal charges and up to 10 years in prison. CHOs covered by HIPAA can face federal investigation, fines, lawsuits, and loss of client trust. Staff could face termination, and agencies may lose licenses or federal funding.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
HUD Vendor Agreements & Data Use Requirements	Contracts and included policy requirements establishing rights regarding HMIS data and ensuring that third parties protect HMIS data. HUD requires CoCs to have agreements in place so that any HMIS software vendors or external partners with access to HMIS data must uphold the same privacy and security standards as other CHOs. These agreements typically detail acceptable uses of the data and forbid unauthorized disclosure or use of client information. The HMIS lead agency is responsible for securing and managing these agreements and monitoring compliance.	Any client-level HMIS data shared with third parties for permissible purposes. The agreement specifies what the data can be used for, how it must be protected, and who has what rights to the data. Typically, it covers: • Data security practices the vendor must follow • Confidentiality rules • Requirements to return or destroy HMIS data following the end of the contractual relationship	HMIS vendors, contractors, and any other external entity that handles HMIS data under an agreement with the CoC or lead agency. This includes: • Software vendors • Cloud hosting companies • Data analysts • Technical assistance providers If an organization or individual outside traditional CHOs will see or use client-level data, they must sign an agreement to comply with all requirements.	Enforced via contracts and oversight. If a vendor or partner violates the vendor agreement or data use requirements, the CoC can and should terminate the contract or access and pursue legal remedies. The vendor could be subject to breach of contract claims and potential liability for damages. Additionally, any data breach or misuse could trigger sanctions under other data privacy protections discussed above. Agreements often include indemnification clauses which require the vendor to cover any costs associated with a violation.

	What Is It?	What Does It Cover?	Who Must Comply?	What If It's Violated?
CoC Governance Charters and Local Policies & Procedures	CoC-level documents include Governance Charters and local HMIS policies, procedures, and data sharing agreements that take federal laws and standards and make them specific to the community, including details on how to obtain consent or what specific data elements are shared. HUD requires each CoC to have a Governance Charter and written HMIS Policies & Procedures, including a Privacy Plan, Security Plan, and Data Quality Plan. These local policies set the detailed rules for HMIS use in the community and often incorporate any stricter state or local laws or norms. CHOs sign an HMIS participation or data sharing agreement that spells out their responsibilities to protect client data. The CoC Board or HMIS governance/data committee is responsible for updating and enforcing these policies.	The specifics of data sharing and security at the local level, such as: • Which client data elements can be shared between providers and which cannot • How an ROI is obtained and documented • Rules for user passwords and other physical security • Rules regarding the retention of data These agreements translate federal requirements into practice and supplement baseline standards with additional protections required by state or local law.	All CHOs and end users within the CoC, including: • The HMIS lead agency • Each agency that enters or views data • Every end user (incl. case managers, data analysts, etc.)	Enforced through monitoring/sanctions by the CoC. If an agency or user violates the local HMIS privacy rules, they can face escalating consequences such as: • Warnings • Retraining, • Suspension or revocation of HMIS access Serious breaches may trigger notification requirements and lead to civil penalties. CHOs whose access to HMIS is revoked risk their funding. Staff who fail to comply with local policies may be terminated.
State and Local Data Privacy Laws	In addition to the federal frameworks discussed above, state and local law may impose additional requirements. **Follow the most protective/restrictive standard applicable**. Safeguarding HMIS data is critical to protecting client safety and privacy, maintaining community trust, and ensuring continued funding and support.			