The following safeguards are required by HUD as specified in their [HMIS Data and Technical Standards](https://www.onecpd.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/) (2004)

**Three County Continuum of Care**

**HMIS Checklist: Privacy, Confidentiality, and Security**



(<https://files.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf>)

# Intake: Privacy, confidentiality, release of information

*HUD requires that all clients for whom HMIS (Homeless Management Information System) data is collected be informed that they have a right to review the organization’s Privacy Policy; that they have the right to refuse to provide information with no impact on their services; and/or that they have the right to refuse to share their information electronically with the CoC.*

*In addition, the organization must make sure that:*

Release of Information to electronically share personal information is signed at intake for each client

Data collection notice is posted where intake interviews occur

Privacy Notice is current and available

HMIS Privacy Policies are posted on website

Hard copies of intakes are stored in locked cabinets

Hard copies containing personally identifiable information are shredded before disposal

# HMIS Operations: Data policies, user agreements, computer security

*HUD technical and security standards require that measures be taken to protect the integrity, security, and confidentiality of HMIS data. After the HEARTH Act is fully implemented, HUD will further require that every participating organization appoint a Security Officer who will be responsible for maintaining the organization’s compliance with security standards. Standards include:*

Formal or informal policy requiring that data be entered into the HMIS within **24 hrs of the entry or exit for emergency shelters**, within **48 hours for rapid re-housing and homelessness prevention programs**, within **72 hours for coordinated access vulnerability assessments, street outreach and supportive services only programs**, and within **120 hours** (**5 days) for permanent and transitional housing projects**

HMIS user agreements are in place

Workstations are located in a secure location

Computers used for HMIS are password protected

Computers used for HMIS have up-to-date antivirus software

Computers used for HMIS have locking screen savers

Computers used for HMIS have an individual or network firewall

Documents containing personally identifiable information are stored in an encrypted or password protected file or on an encrypted drive in a computer which meets all of the above conditions