SECURITY

QUICK FACT OVERVIEW

HMIS San Antonio/Bexar County
Homeless Management Information System

Contact HMIS
HMIS.Support@HavenForHope.org

ALL AUTHORIZED HMIS USERS

- No unauthorized users are permitted to view or access HMIS (including new employees shadowing on the job prior to attending HMIS New User Training).
- HMIS workstations are password protected and locked when not in use.
- HMIS password is kept secure and not stored to browser.
- Documents printed from HMIS are kept in a secure location.
- Unencrypted PHI is never electronically transmitted in any fashion, including via email and through the HMIS Ticketing System.
- Client profiles are only searched on a need-to-know basis.
- Never sign in using someone else's credentials.
- HMIS Security Awareness Agreement requires annual renewal.

AUTHORIZATION CONTACTS

- Notifies HMIS within 24 hours of employee termination or resignation to prevent unauthorized access.

ORGANIZATION RESPONSIBILITIES

- All HMIS workstations have antivirus software.
- All HMIS workstations have an individual or network firewall.
- Privacy Notice is posted in a visible area where intakes take place.

PROTECTING CLIENT PRIVACY & CONFIDENTIALITY

- Release of Information (ROI) must be on file.
- Omit all PHI from unencrypted correspondence, including tickets submitted to HMIS.

PROTECTED HEALTH INFORMATION (PHI) IDENTIFIERS

- Name
- Postal Address
- All elements of dates except year (ex: DOB)
- Telephone Number
- Fax Number
- Email Address
- URL Address
- IP Address
- Social Security Number
- Account Numbers
- Certificate/Licenses Number
- Medical Record Number
- Health Care Beneficiary Number
- Device Identifiers & serial numbers
- Vehicle Identifiers & serial numbers
- Biometric Identifiers (finger & voice prints)
- Full Face Photos & Other Comparable Images
- Any other unique identifying number, code, or characteristic