

HMIS

(HOMELESS MANAGEMENT INFORMATION SYSTEM)
SECURITY AWARENESS TRAINING

Created By:



Revised: 1/07/2019

Overview

- ❑ The purpose of this presentation is to emphasize the importance of security when using HMIS. Client information is confidential and should always be treated as such. **This presentation provides an overview for the following topics:**
 - ❑ HUD HMIS Data Standards
 - ❑ Basic Requirements
 - ❑ User Authentication/Access
 - ❑ Defining Security
 - ❑ Client Confidentiality
 - ❑ HIPAA

HUD's HMIS Data Standards

- ❑ The purpose of the data standards are to *“ensure that every HMIS captures the information necessary to fulfill HUD reporting requirements while protecting the privacy and informational security of all homeless individuals.”*
- ❑ The most recent version is April 2018.
- ❑ **You may access these data standards at:**

<https://www.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf>

Basic Security Requirements

- ❑ **HMIS Users Need:**
 - ❑ Unique username and password
 - ❑ Signed Electronic Security Awareness Agreement (digital copy in HMIS)
 - ❑ Security Awareness valid for 365 days
- ❑ **Each Computer/Network Needs:**
 - ❑ A secure location
 - ❑ Anti-virus software
 - ❑ Individual or network firewall

Username and Password

- ❑ Every user accessing HMIS must have a unique username and password
- ❑ A unique password includes:
 - ❑ At least 1 number
 - ❑ At least 1 lowercase letter
 - ❑ At least 1 capital letter
 - ❑ At least 6 characters long
 - ❑ At least 1 special character
 - ❑ Good: [Na\$car#39]
 - ❑ Bad: Pass.1

HMIS access

- ❑ Users are assigned a role in the HMIS application. A role defines how much information and the type of information you can access. Your agency and the HMIS Manager will determine your role access.
- ❑ HMIS is built to automatically log you out if there is inactivity beyond 30 minutes.
- ❑ Log out of HMIS when away from the workstation.
- ❑ **Do not** share your login information with anyone!

Physical Access / Location

- ❑ **Secure workstations**
- ❑ (It is your responsibility for good computer practices)
 - ❑ Lock offices
 - ❑ Place computer monitors away from others' view
 - ❑ Use a privacy screen when necessary
 - ❑ Lock computer screens when away from the workstation (windows logo key + L)



Uses of HMIS

- ❑ **HMIS should not be used for:**
 - ❑ Personal gain
 - ❑ Bias opinions
 - ❑ Stalking
 - ❑ Sharing with others outside of service providers
 - ❑ Curiosity
- ❑ **HMIS should be used for:**
 - ❑ Tracking enrollments/assessments
 - ❑ Referring clients
 - ❑ Creating case notes
 - ❑ Coordinating services for a client

Defining Security

- ❑ **Security** refers to the protection of clients' personal protected information and sensitive program information from unauthorized access, disclosure, use, or modification.



Client Confidentiality

- ❑ Agencies and Individual Users of HMIS are required to comply with federal, state, and local confidentiality laws
- ❑ Agencies and Users are required to comply with limits to data collection (relevant, appropriate, lawful)
- ❑ Agencies are required to post sign at intake or comparable location with general reasons for information collection and reference to privacy policy
- ❑ Agencies may infer consent for uses in the posted sign and written privacy policy

Protecting Clients Privacy

- ❑ **Client information should only be shared/searched on a need-to-know basis.**
 - ❑ **Need-to-know:**
 - ❑ 1. The **legitimate** requirement of a person to access sensitive information that is **critical** to the performance of an **authorized, assigned mission in connection with services to a client.**
 - ❑ 2. The **necessity** for access to specific information required to carry out official duties.
- ❑ **HMIS Team monitors individual HMIS use. User must be able to support access to client's file.**
- ❑ **Violations must be reported to the Security Manager, Haven for Hope HIPAA Officer, in some cases, to government agencies and the Client.**
- ❑ **Violations may result in termination of use rights, disciplinary action, and in extreme cases, prosecution.**

Privacy and Security Laws

- Federal Health Insurance Portability and Accountability Act (HIPAA, 1996)
- Texas Medical Records Privacy Act (MRPA, 2012)
- 42 CFR Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records (HHS)

WHAT IS HIPAA?

- ❑ The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - ❑ The HIPAA Rules apply to “Covered Entities” and “Business Associates” .
 - ❑ Covered Entities include certain health care providers, health plans, and health care clearing houses.
 - ❑ Hospitals & Health Clinics
 - ❑ Some mental health & substance abuse treatment programs
 - ❑ A Business Associate is any person or entity that:
 - ❑ Performs an activity or function on behalf of a covered entity that involves Protected Health Information (**PHI**), OR
 - ❑ Provides legal, accounting, management, administrative, financial, or other services for a covered entity that involves PHI.

What Information Must Be Protected?

- ❑ You must protect an individual's Protected Health Information (**PHI**) which is collected or created as a consequence of providing care. These rules apply to you when you view, use, and share PHI.

- ❑ **PHI:**

- ❑ Is information related to a patient's past, present or future physical and/or mental health condition
- ❑ Can be in any form: written, spoken, or electronic
- ❑ Includes at least one of the 18 identifiers:

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
- ❑ Certificates/Licenses number
- ❑ Medical record number
- ❑ Health care beneficiary #
- ❑ Device identifiers and their 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

Disclosures of PHI

May be disclosed:

- ❑ With written consent, or
- ❑ If required by court order, or
- ❑ In a medical emergency, or
- ❑ For research, audit, or program evaluation
- ❑ To another health care provider for purposes of Treatment, Payment, or health care Operations (**TPO**) (e.g. to a partner, physician, or hospital)

Disclosures of PHI

- ❑ To the client
- ❑ In accordance with client's written authorization
- ❑ To a client's legal representative or a family member involved in client care
- ❑ To report child abuse or neglect, abuse of an adult, or domestic violence
- ❑ Haven for Hope considers that other disclosure is non-routine and requires approval by the Haven for Hope HIPAA Privacy Officer

Keep in Mind

- Use PHI only as necessary to perform your job duties
- Use & disclose the minimum necessary to perform job duties
- If you need to use or disclose PHI outside of routine uses/disclosures, **please consult the Haven for Hope Attorney/HIPAA Privacy Officer first**

Haven for Hope Attorney & HIPAA Privacy Officer:

Brooke Holland (210) 220-2183

Brooke.Holland@havenforhope.org

HMIS Security Officer:

David Huete (210) 220-2352

David.Huete@havenforhope.org

Read & Sign Digital Copy

AGENCY/ORGANIZATION NAME: _____

LOCATION: _____

San Antonio Homeless Management Information System (HMIS)

USER CONFIDENTIALITY AGREEMENT

I understand that I will be allowed access to confidential information and/or records in order to perform my specific job duties. I further understand and agree that I am not to disclose such confidential information and/or records without the prior consent of the appropriate authority(s).

I understand that all USERID/ Passwords to access the HMIS are issued on an individual basis. I further understand that I am solely responsible for all information obtained, through system access, using my unique identification. At no time will I allow any other person to use of my USERID/Password to logon to the HMIS. I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released except as allowed in the HMIS Security Awareness training, outside the scope of my assigned job duties would constitute a violation of this agreement. I understand my supervisor will be notified immediately of any violation and disciplinary action will be taken, up to termination of employment.

By affixing my signature to this document I acknowledge that I have been apprised of the relevant laws concerning access, use, maintenance and disclosure of confidential information and/or records available to me through my use of the HMIS. I further agree that it is my responsibility to assure the confidentiality of all information I access through use of HMIS, even after my access to HMIS has ended.

Pursuant to this agreement I certify that I have read and understand the laws concerning confidential information and/or records and the HMIS Security Awareness Training materials.

User Signature _____ **Date** _____ **Job Title** _____

Print User Name _____ **Email** _____