MA-503 CAPE COD AND ISLANDS CONTINUUM OF CARE

HMIS SECURITY TRAINING 12/1/2021

TRANSCRIPT

SLIDE 1

Welcome to the Cape Cod and Islands Continuum of Care Security Training for Users of the Homeless Management Information System (HMIS).

SLIDE 2

DEFINITIONS AND ABBREVIATIONS - Some of the terms and abbreviations that will be used in this presentation are:

Continuum of Care (CoC) - a regional or local planning body that coordinates housing and services for homeless families and individuals. The US Department of Housing and Urban Development provides funding for the Cape Cod and Islands CoC.

Covered Homeless Organization (CHO) – Any organization that records, uses, or processes Personally Identifiable Information on homeless clients for an HMIS.

Homeless Management information System (HMIS) – An HMIS is a local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness.

Personally Identifiable Information (PII) – PII is information that can be used to distinguish an individual's identity, either alone or when combined with other identifying information linked to a specific individual. Common examples of PII include name, address, date of birth, Social Security Number, etc.

US Department of Housing and Urban Development (HUD) - The Department of Housing and Urban Development is the Federal agency responsible for national policy and programs that address America's housing needs. HUD administers the Continuum of Care Program, under which the Cape Cod and Islands CoC operates.

WellSky / Servicepoint - Servicepoint is the name of the software product used for the CoC's HMIS. WellSky is the vendor of Servicepoint. Servicepoint and HMIS are not synonymous: Servicepoint is the software, HMIS is the function.

SLIDE 3

WHAT ARE DATA PRIVACY AND DATA SECURITY?

Frequently the terms **data privacy and data security are** used interchangeably. However, the two concepts are not exactly the same. **Data privacy** is concerned with **the proper handling, processing, storage, and usage of personal information.** Data privacy concerns revolve around:

(1) Whether or how data is shared with third parties
(2) How data is legally collected or stored
(3) Regulatory restrictions such as HIPAA

Data security means protecting **personal data** from any unauthorized third-party access or malicious attacks and exploitation of data. Data security is set up to protect personal data using different methods and techniques to ensure data privacy. Data security ensures the **integrity of the data**, meaning data is accurate, reliable, and available to authorized parties only.

SLIDE 4

WHO ESTABLISHED DATA SECURITY STANDARDS?

The US Department of Housing and Urban Development (HUD) requires that client level HMIS data be safeguarded and protected from unauthorized access. The privacy and security standards as described in the **2004 HMIS Data and Technical Standards Notice** seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data.

The **Continuum of Care Interim Rule** states that the Continuum of Care must designate and operate the HMIS and must review, revise, and approve a privacy plan, a security plan, and a data quality plan for the HMIS.

SLIDE 5

WHY DO USERS NEED HMIS SECURITY TRAINING?

In addition to Federal regulations, the Cape Cod and Islands HMIS Policies and Procedures require that all users be trained to observe and practice the levels of confidentiality and security mandated by HUD.

All users must receive security and privacy training prior to being given access to the HMIS and being issued a password. The request for new password requires a certification that the new user has completed the on-line training.

SLIDE 6

CAPE COD AND ISLANDS HMIS SECURITY PLAN – Federal regulations require each CoC to establish an HMIS Data Security Plan that is incorporated into the HMIS Policies and Procedures. The outline of the Cape Cod and Islands CoC HMIS Security Plan will be discussed during the remainder of the presentation.

1] HMIS SYSTEM SECURITY OFFICER

The Cape Cod and Islands HMIS System Administrator serves as the HMIS System Security Officer, whose duties include:

- Reviewing the Security Plan annually or anytime there is a change to the security requirements
- Confirming that the Cape Cod and Islands CoC HMIS adheres to the Security Plan
- Responding to any security questions, requests, or security breaches related to HMIS and communicating security-related information to CHOs

[2] CHO SECURITY OFFICER

Each CHO must also designate a CHO Security Officer whose duties include:

- Confirming that the CHO adheres to the Security Plan
- Communicating to the HMIS System Administrator any:
    - security questions
    - requests
    - security breaches
    - security-related information conveyed by the CHO's end users
- Participating in annual security trainings offered by the Cape Cod and Islands CoC
- Completing an annual security review. Each CHO must complete a security checklist ensuring that all security standards are implemented in accordance with the HMIS security plan. The completed form should be submitted to the HMIS System Administrator by February 15 of each year.

SLIDE 7

[3] REPORTING SECURITY INCIDENTS

All HMIS users must report to their CHO Security Officer:

- Suspected instances of noncompliance with policies and procedures that may leave HMIS data vulnerable to intrusion
- Any incident in which unauthorized use or disclosure of PII has occurred
- Any incident in which PII may have been used in violation of HMIS Privacy and Security Policies
- Any other type of security violation

The CHO Security Officer must report violations to the HMIS System Administrator, who will review violations and recommend corrective and disciplinary actions to the CHO as appropriate.

[4] AUDIT CONTROLS

The HMIS System Administrator will monitor audit reports in HMIS for any apparent security breaches or behavior inconsistent with the Privacy and Security Policies outlined in these policies and procedures.

SLIDE 8

[5] SYSTEM SECURITY

Each CHO must apply system security provisions to all the systems where PII is stored, including, the CHO's networks, desktops, laptops, mini- computers, mainframes and servers.

Each CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must meet reasonable industry standard requirements.

Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

[6] VIRUS PROTECTION

A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

[7] FIREWALLS

A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

[8] PHYSICAL ACCESS

A CHO must ensure that computers used to collect and store HMIS data and that are stationed in public areas are staffed at all times. When workstations are not in use and staff are not present, computers and data must be secured and not usable by unauthorized individuals. Workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Staff should log off the data entry system and shut down the computer whenever leaving the workstation for an extended period of time.

SLIDE 9

[9] HARD COPY SECURITY

A CHO must secure any paper or other hard copy containing PII that is generated by or for HMIS, such as reports, data entry forms, and signed consent forms. A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, must be treated in the following manner:

(1) Records should be kept in individual locked files or in rooms that are locked when not in use
(2) When in use, records should be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record
(3) Employees should not remove records or other information from their places of business without permission from appropriate supervisory staff
(4) When staff remove records from their places of business, the records must be maintained in a secure location and staff must not disclose the PII contained in those records
(5) Faxes or other printed documents containing PII must not be left unattended
(6) Fax machines and printers must be kept in secure areas
(7) When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt
(8) When finished faxing, copying, or printing, staff should immediately remove all documents containing PII from the machines

SLIDE 10

[10] DATABASE INTEGRITY

The CHO must not intentionally cause corruption of the Cape Cod and Island HMIS in any manner. Any unauthorized access or modification to computer system information, or interference with normal system operations, will result in immediate suspension of HMIS licenses held by the CHO, and suspension of continued access to the Cape Cod and Islands HMIS by the CHO.

The CoC will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be subject to sanctions and to disciplinary action by the employer CHO.

[11] DISASTER RECOVERY

The CoC's HMIS data is stored by WellSky in secure and protected off-site locations with duplicate back-up. In the event of disaster, the HMIS System Administrator will coordinate with

WellSky to ensure that the HMIS is operational and that data has been restored. The CoC will communicate to CHOs when data becomes accessible following a disaster.

[12] CONTRACTS AND OTHER ARRANGEMENTS

The Massachusetts Department of Housing and Community Development (DHCD) is the Administrator of the Massachusetts Rehousing Data Collective (RDC), a statewide data warehouse in which the CoC participates. DHCD will retain copies of all contracts and agreements necessary to comply with HUD requirements.

[13] DATA COLLECTION NOTICE

Agencies that contribute HMIS data must let clients know that PII is being collected and the reasons for taking this information. The CoC's HMIS Policies and Procedure manual contains a sample Notice that covers the minimum requirement.

SLIDE 11

[14] PRIVACY NOTICE

Each agency is required to publish and post on its web site a Privacy Notice describing its policies and practices for use of PII and must provide a copy of its Privacy Notice to any individual upon request. Sample Privacy Notices in English and Spanish may be found in the CoC's HMIS Policies and Procedures manual.

[15] ACCOUNTABILITY

Agencies must require staff to sign an agreement that acknowledges receipt of a copy of the Privacy Notice and that pledges to comply with the Privacy Notice.

Each CHO must establish a written policy for accepting and considering questions or complaints about its privacy and security policies and practices.

[16] ACCESS AND CORRECTION

In general, agencies must allow clients to inspect and to have a copy of their information and must offer to explain any information that clients may not understand. Agencies must consider requests by clients for correction of inaccurate or incomplete information but are not required to remove any information. However, the agency may mark information as inaccurate or incomplete and may supplement it with additional information.

The agency may deny access to PII for any of the following reasons, and should describe possible reasons in its Privacy Notice:

(1) Information compiled in reasonable anticipation of litigation

(2) Information about another individual

(3) Information obtained under a promise of confidentiality if disclosure would reveal the source of the information

(4) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

The agency can reject repeated or harassing requests for access or correction. An agency that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the PII about the individual.

SLIDE 12

[17] PURPOSE AND USE LIMITATIONS

Agencies may use or disclose PII from HMIS under the following circumstances:

(1) For the provision or coordination of services to an individual
(2) For functions related to payment or reimbursement for services
(3) For carrying out administrative functions, including but not limited to legal, audit, personnel, oversight, and management functions
(4) For creating de-identified PII

Certain disclosures of PII may be required that go beyond the privacy interests of clients. The following additional uses and disclosures are described in detail in the HUD 2004 HMIS Technical Standards:

(1) Uses and disclosures required by law
(2) Uses and disclosures to avert a serious threat to health or safety
(3) Uses and disclosures about victims of abuse, neglect, or domestic violence
(4) Uses and disclosures for academic research purposes
(5) Disclosures for law enforcement purposes

SLIDE 13

[18] CONFIDENTIALITY

Each CHO must develop and implement written procedures to ensure that:

(1) All records containing PII will be kept secure and confidential
(2) The address or location of any family violence project will not be made public, except with written authorization of the person responsible for the operation of the project
(3) The address or location of any program participant will not be made public, except with authorization of the participant and consistent with State and local laws regarding privacy and obligations of confidentiality.

[19] VICTIM SERVICES

Victim service providers are prohibited from entering data into HMIS and must maintain a separate, comparable database. Additional protections for these survivors of domestic violence include explicit training for staff handling PII of the potentially dangerous circumstances that may be created by improper release of this information.

SLIDE 14

[20] OTHER REQUIREMENTS

All agencies that contribute HMIS data must comply with the baseline privacy requirements described in this Privacy Plan. CHOs must also comply with federal, state and local laws that require additional confidentiality protections. If a CHO's privacy or security standard conflicts with other Federal, state, and local laws, the CHO must update their policies to accurately reflect the additional protections.

[21] ELECTRONIC COMMUNICATION

Email is a vulnerable medium, particularly when emails are sent over unsecured Wi-Fi networks. Even emails sent within a secure agency network can be intercepted by other users. Email encryption involves encrypting, or disguising, the content of email messages in order to protect PII from being read by anyone other than intended recipients. Encryption renders the content of your emails unreadable as they travel from origin to destination, so even if someone intercepts your messages, they can't interpret the content. Encryption is available through numerous email programs, including Gmail and Outlook. If you are uncertain about your agency's email encryption capabilities, check with your IT department.

SLIDE 15

CERTIFICATION OF ATTENDANCE

Prior to being issued a username and password to access HMIS for the first time, it is necessary to notify the HMIS System Administrator via email that you have completed this virtual HMIS Security Training. Please include your name, your agency, your job title, and the date on which you completed the training, and send the email to martha.taylor@barnstablecounty.org.

SLIDE 16

QUESTIONS

If you have questions or need more information, please contact Martha Taylor, HMIS Program Manager, at martha.taylor@barnstablecounty.org or call 508-375-6625.