IN BOS Continuum of Care
HMIS Security and Privacy Policies for HMIS
Approved October 27, 2016 – Effective January 1, 2017

• All agencies must comply with the current HMIS Privacy, Confidentiality, and Security standards issued in the HUD Notice on 7/31/2004. These standards may change during the grant year, but currently require, but are not limited to:
  a. Installing virus protection software, with an automatic update on every computer that accesses HMIS
  b. Utilize any supported operating system (windows 7 and above) and keep up-to-date on operating system updates
  c. Activating a locking screen saver on every computer that accesses HMIS
  d. Posting the HMIS privacy notice (long version) on its agency website
  e. Installing an individual and/or network firewall
  f. Posting “Privacy Notice” signs at each intake desk

• Documentation of client refusal must be maintained in each consumer file. Individuals refusing to authorize participation in HMIS should be discussed with the HMIS Manager. An ID number will be assigned to document equivalent HMIS data elements to be gathered and documented in the case file.

• IHCDA staff and HMIS contractors will monitor HMIS participation through periodic desk and/or onsite monitoring, in addition to ongoing review of data in the HMIS. Data will also be reviewed within the monitoring & claims process for HUD sponsored housing programs. IHCDA reserves the right to withhold payment until HMIS violations are corrected or required levels of data quality are achieved. For example, violations include, but are not limited to a percentage of “Missing” or “Don’t Know/Refused” responses for universal data elements above 5% for any element.

• Agencies must respond to IHCDA in writing when notified of HMIS Policy Violation within 10 working days of receipt. Agencies should inform IHCDA of how they have responded to the violation. Failure to comply with HMIS requirements may result in IHCDA withholding payments until compliance is complete and documented, or termination of the grant(s). In addition, failure to comply with requirements may result in an agency being ineligible for funding or receiving a low HMIS performance score in the next grant year.

Privacy Policy
IHCDA and IN BOS CoC will not sell or rent personally identifiable information that we collect, and will not collect or share personally identifiable information.
Log Files: IHCDA and HMIS contractors may use IP addresses to analyze trends, administer the site and gather broad demographic information for aggregate use.
Security Policy
IHCDCA and HMIS contractors take every precaution to protect the information of clients. When you submit sensitive information via the HMIS, your information is protected both online and off-line. When HMIS/DV ClientTrack users are asked to enter sensitive information (such as a social security number) the information is encrypted. While on a secure page, the lock icon on the bottom of web browsers such as Mozilla Firefox and Microsoft Internet Explorer becomes locked, as opposed to un-locked, or open, when you are just ‘surfing’. While we use SSL encryption to protect sensitive information online, we also do everything in our power to protect client information off-line. All of our client information, not just the sensitive information mentioned above, is restricted. Only IHCDCA and HMIS contractors and authorized Community Service staff at IHCDCA who need the information to perform a specific job are granted access to personally identifiable information. The servers that we store personally identifiable information on are kept in a secure environment, with the state Information Office of Technology (IOT).

The use of HMIS/DV ClientTrack constitutes an express consent to the monitoring of system use and security at all times. If such monitoring of HMIS/DV ClientTrack reveals possible violations of the law, pertinent information will be provided to law enforcement officials. Any persons using HMIS or information obtained from this application, without proper authorization or in violation of these policies and procedures may be subject to civil and/or criminal prosecution. Any persons enabling access by an unauthorized individual may also be subject to internal disciplinary actions in addition to civil and/or criminal prosecution.

These policies are applicable to all HMIS/DV ClientTrack users (employees, contractors, and others) of agencies, partners and funders and the computer systems, networks, and any other electronic processing or communications and related resources used in conjunction with the IHCDCA HMIS system and/or data obtained through the HMIS system.

IHCDCA and HMIS contractors place highest priority on the security of its systems, and the private information they contain. IHCDCA and HMIS contractors continually work to protect data and systems:
1. Confidentiality. Access to client information must be tightly controlled and people with access to confidential information must understand their personal responsibility to maintain its confidentiality.
2. Integrity. Client information must be protected so that it cannot be modified while in transit or storage. Reported data must be accurate.
3. Availability. Systems must be available to users when and where they need them. If an employee leaves your agency, inform IHCDCA and HMIS contractors within 24 hours so that their account can be deactivated.

Information Security Procedures:
All IHCDCA and HMIS contractors’ employees are responsible for protecting the confidentiality and security of HMIS data systems and the human services client information they contain. Information concerning the security related tasks an employee is responsible for are included in the employee’s job description. The agency is responsible for ensuring that information that is printed from the HMIS is also kept confidential, private and secure.

Data Sharing across Providers
At point of service the client may authorize an agency to access existing information in the HMIS, and to add information about the client to the HMIS. When the client approaches another organization, the authorization process is repeated. This ensures that no agency accesses a client’s record without that client’s specific permission, and it significantly increases client confidence in the HMIS. The Regional
Administrators have signed MOUs that allow for data sharing across agencies, but this is limited to aggregate data (currently we do not have regional administrators).

Data Disposal
Removable drives/devices/laptops/desktops/thumb drives and any other electronic media or equipment will be disposed of by means of physical destruction and/or wiping/magnetization for erasure before disposal. Hard copy info must be shredded or securely deleted all identifying information.

Coordinated Entry
A client consent will be required as part of the Coordinated Entry process. A client consent will be good for 3 years. This will allow all HMIS participating agencies to access client info regardless of agencies HIPAA obligations. At point of service the client may authorize an agency to access existing information in the HMIS, and to add information about the client to the HMIS. When the client approaches another organization, the authorization process is repeated. This ensures that no agency accesses a client’s record without that client’s specific permission, and it significantly increases client confidence in the HMIS.

“Protected” Information
Protected Agency: Certain agencies that deal substantially with HIV/AIDS, domestic violence, substance abuse, mental illness, or legal services are designated as Protected Class agencies. If your agency is a Protected Class agency, all Client Services Information records (including referrals) are hidden, or protected, from view by any other agency. Basic client information will still be accessible to other agencies.

Access to Data for Monitoring
IHCDA, as the lead HMIS agency, will have limited access to your agency’s data for monitoring purposes and aggregate reporting purposes. All IHCDA HMIS staff and HMIS contractors who have access to data will undergo Confidentiality and Ethics training.

Unauthorized Access to the IHCDA system:
Any user accessing the HMIS system must be affiliated with an active member agency. Additionally, each system user must attend the required user training, have completed a new User HMIS Agreement Form in order to be given a User Id and Password. Unauthorized access is prohibited and is grounds for legal action. Users must also attend annual security and confidentiality training in order to remain active users.

Client Grievances
Grievance Procedure:
- A client has the right to appeal his or her individual complaints related to their HMIS data to the entering agency in accordance with the agency’s established grievance policy.
- Complaints about the conduct or practice of HMIS may be filed in writing to the HMIS Manager at IHCDA.
- Agencies are responsible for establishing an internal grievance process to handle client complaints and grievances related to consent and release of information related to the HMIS system. If a client has a grievance regarding erroneous data entry or inappropriate use of their data, they will need to follow the agency’s established guidelines, standard operating procedures or protocol on resolving these issues.

Revoking Authorization: