TBIN Audit Plan

Created: 11-2016
Updated:

Tampa Bay Information Network

TBIN Audit Plan

Table of Contents

Introduction

The Homeless Management Information System (HMIS) Lead Agency is responsible for overseeing the privacy and security of personal information collected and stored in an electronic form for all Participating Member Agencies, as stated in the HMIS Data and Technical Standards (69 Federal Register 45888) released in 2004 and in the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) HMIS Proposed Rule (76 Federal Register 76917) released in 2011 by the U.S. Department of Housing and Urban Development (HUD). These standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of the data between the HMIS Lead Agency, Participating Member Agencies, and Non-Participating Organizations. The 2004 HMIS Data and Technical Standards are currently the baseline requirements for any HMIS System.

The Tampa Bay Information Network (TBIN), the HMIS system for Pinellas County Continuum of Care, is administered by 2-1-1 Tampa Bay Care, Inc. (211 TBC). 211 TBC is the HMIS Lead Agency for Pinellas County. The Pinellas County Homeless Leadership Board, Inc. (HLB) is the Continuum of Care (CoC) Lead Agency.

This Audit Plan outlines the rules, responsibilities, and processes for monitoring compliance of the 2004 HMIS Data and Technical Standards between TBIN and TBIN Member Agencies. All data entry users and administrators of TBIN Member Agencies must adhere to this Audit Plan. Privacy and security of client information is of critical importance to all data entry users and administrators of TBIN Member Agencies. Additionally, this audit plan describes how TBIN will monitor compliance requirements established in the HMIS Data and Technical Standards.

The goal of TBIN is to provide a centralized shared basic needs client information system to be used for intake and case management at local social service organizations.

This audit plan has been developed by the TBIN staff and approved by the HLB Board of Directors.

Definitions & Acronyms

Agency Administrator (AA) - The lead user at a TBIN Member Agency with some advanced reporting and administrative rights within the TBIN system.

Covered Homeless Organization (CHO) - Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PII on homeless clients for an HMIS.

Homeless Management Information System (HMIS) - Is the information system designated by a local CoC to comply with the requirements of CoC Program interim rule 24 CFR 578. It is a locally-administered data system used to record and analyze client, service and housing data for individuals and families who are homeless or at risk of homelessness.

Personal Identifiable Information (PII) - Any information maintained by or for a Covered Homeless Organization about a homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) Can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Privacy - Is the ability to confidentially protect Personal Identifiable Information (PII) captured about a client to prevent unauthorized viewing or access to such information.

Security – Is the means that is used to maintain the privacy of collected PII about a client. This could entail administrative safeguards, physical safeguards, and technical safeguards that ensure that PII is not accessible to unauthorized persons.

TBIN Member Agency - A participating and compliant organization who enters data into the TBIN system.

User - Employees, volunteers, affiliates, contractors, and associates at a TBIN Member Agency who directly enters and manages client records in the TBIN system.

Documents

Document	Description	Use	Location
Privacy Notice	This document describes what and why a CHO collects, manages, reports, and discloses client information.	*REQUIRED* Agencies must publicly post this privacy notice.	www.tbin.zendesk.com TBIN Forms, Guides, Policies > Forms
Client Informed Consent	This form explains to the client of what and why a CHO collects, manages, reports, and discloses client information. The clients sign that they have read and agree to share.	*REQUIRED* Agencies must present this form for clients to read and sign, at minimum, every three years.	www.tbin.zendesk.com TBIN Forms, Guides, Policies > Forms
Client Release of Information	This form gives the client control to assign who sees their information and what information is shared with other CHO's.	*REQUIRED ONLY IF CONSENT NOT COMPLETED* Agencies must present this form and the clients must assign access to their record and sign permission to access their data.	www.tbin.zendesk.com TBIN Forms, Guides, Policies > Forms
TBIN Audit Form	This Form outlines the requirements of a CHO concerning privacy, security and HMIS standards.	*REQUIRED* Agencies must adhere to this Form and must correct any issues reported during the audit process.	www.tbin.zendesk.com TBIN Forms, Guides, Policies > Coming Soon
TBIN Policies and Procedures	This document explains the rules and requirements of all CHO's that access the TBIN system.	*REQUIRED* Agencies must adhere to this document.	www.tbin.zendesk.com TBIN Forms, Guides, Policies > Policies

Purpose

The goal of the TBIN Audit Plan is to ensure confidentiality and security of all client data captured in TBIN conforms to all current regulations related to privacy, security and HMIS standards. Outlined in this audit plan are clear guidelines and procedures that will be followed by TBIN and TBIN Member Agency to ensure compliance with HMIS standards. Auditing will be the means by which TBIN will have documented quality assurance that all TBIN Member Agencies are in compliance of the HMIS standards.

Guidelines

Each participating TBIN Member Agency will be required to conform ~~with~~ to all sections of this Auditing Plan. The following sections are a brief overview of Privacy, Security, Data Quality, Data Timeliness and HMIS Standards. At least annually, TBIN staff will be onsite at every TBIN Member Agency data entry or client intake location, to perform an audit of all components that are described in this plan. Any TBIN Member Agency that does not allow time for the TBIN staff to perform the audit process could forfeit agency access to the TBIN system. Any TBIN Member Agency that does not correct issues identified during the TBIN Audit ~~in a timely manner~~in the timeline submitted within the Audit findings, could forfeit all access to the TBIN system.

Privacy

Privacy is the ability to confidentially protect Personal Identifiable Information (PII) which is any information maintained about a client that:

a. Allows identification of a client/consumer directly or indirectly
b. Can be manipulated by a reasonably foreseeable method to identify a specific client/consumer, or
c. Can be linked with other available information to identify a specific client/consumer.

Client Consent: TBIN Member Agencies may be required to collect PII by law or by contract from organizations that fund the operations of the agency. PII is also collected by TBIN Member Agencies to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. TBIN Member Agencies are permitted to collect PII only with a client's written consent. Written permission must be obtained on one (both are not required) of the following forms signed by the client:

- Informed Consent ***(For more information please see the TBIN Policy and Procedure at www.tbin.zendesk.com.)***
- Release of Information (ROI) ***(For more information please see the TBIN Policy and Procedure at www.tbin.zendesk.com.)***

Privacy Notice: By law, TBIN Member Agency providers are required to post a Privacy Notice that discloses collection and use of Client Information. TBIN has developed a document that addresses the collection and use of Client Information. TBIN Member Agency providers must post a TBIN Privacy Notice prominently on their websites and in areas of plain view of the public, such as waiting rooms, intake areas, lobbies, and screening or assessment areas. TBIN Member Agency providers are required to provide a copy of the TBIN Privacy Notice to all clients upon request by the client. ***(For more information please see the TBIN Policy and Procedure at www.tbin.zendesk.com.)***

Removing TBIN User Access: All requests for changes in a TBIN user's license should be communicated to the TBIN staff within 24 business hours after the TBIN user has left the employment of the TBIN Member Agency, the TBIN user has changed positions and is no longer in need of TBIN access, or has knowingly breached or is suspected of a system breach where client data has been compromised. ***(For more information please see the TBIN Policy and Procedure at www.tbin.zendesk.com.)***

Security

In order to protect client privacy, it is important that the following safeguards are put in place for all TBIN Member Agencies. Failure to comply with any of the items listed in this section could forfeit agency access to the TBIN system.

Administrative Safeguards

Background Checks: Each TBIN user at the Member Agency must have completed and passed a level 2 background check prior to attending his or her first TBIN training to ensure that clients are protected from fraud or Identity theft. ***(For more information regarding background checks please see the TBIN Policies and Procedures at www.tbin.zendesk.com.)***

TBIN Member Agency Security Officer: All TBIN Member Agencies must designate a Security Officer to be responsible for ensuring compliance with applicable security standards. The security officer, may be the TBIN Member Agency Administrator or another Agency employee, volunteer or contractor who has completed TBIN Privacy and Security training, and will conduct workforce security measures, ensure that each user completes security training at least annually and make sure that a TBIN Audit is completed at least annually. Responsibilities of TBIN Member Agency Security Officers include:

~~1. May be the TBIN Member Agency Administrator or another Agency employee, volunteer or contractor who has completed TBIN Privacy and Security training.~~

~~2.~~1. Conducting a security audit for every workstation that will be used for HMIS entry
   a. prior to issuing a User ID to a new HMIS End User, AND
   b. anytime an existing user moves to or uses a new workstation.

~~3.~~2. Continually ensures each workstation within the Member Agency used for TBIN data entry is protected by all items described in the Technical Safeguards section,

~~4.~~3. Insuring all issues listed in the TBIN Audit Form are either resolved or a corrective action plan has been set in place within 15 business days of the audit.

Physical Safeguards

Computer Location: A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The HMIS workstation must not be accessible to clients, the public, or other unauthorized Partner Agency staff members or volunteers.

Printer location: Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.

PC Access (visual): Non-authorized persons should not be able to see a TBIN workstation screen. Monitors should be turned away from the public or other unauthorized Agency staff or volunteers and utilize visibility filters to protect client privacy. Blackout screens for monitors ~~could~~ should be used in situations where unauthorized persons walk past workstations periodically.

PII Storage: All Member Agencies must have policies and procedures in place that cover storage of Personal Identifiable Information (PII) documentation. Documents containing PII must be stored in a locked area and cannot be left out where unauthorized persons can view or have access to these documents.

PII Disposal: All Member Agencies must have policies and procedures in place that cover the disposal process of hard copy and electronic material that PII is stored on. Documents or electronic media containing Personal Identifiable Information (PII) must be disposed of properly. Paper documents must be shredded or the personal identifiers must be removed from the documents before disposing. All electronic devices (disks, CD's, computer hard-drives, tapes, jump drives, etc.) must be reformatted demagnetized or destroyed before disposing.

Technical Safeguards

Workstation Security

Approved Workstations: To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations by the TBIN Member Security Officer.

User Authentication: All workstations that connect to TBIN must require a username and password to login. The username and password cannot, at any time, be shared among users or with unauthorized users. All users must lock workstations (holding down the control, alt and delete keys and then clicking lock this computer) when leaving their desk for any period of time.

Automatic Locking: All workstations must have automatic locking enabled. Automatic Locking will allow the computer to lock and require a password after being left unattended. This is to prevent unlocked and unattended workstations from being accessible to unauthorized people when left unattended.

Network Security

Firewall: All workstations accessing TBIN must have a current/up to date hardware or software firewall. The internal network must be secure to prevent unauthorized access.

Wi-Fi: All devices that access TBIN remotely through a Wi-Fi connection must use a secured Wi-Fi network. **IT IS STRICTLY PROHIBITED TO ACCESS TBIN USING AN UNSECURE NETWORK AT ANY TIME.** This includes any free Wi-Fi access that does not require a password to gain access to the network (Starbucks, McDonalds, etc.).

Data Access Policy: If the Agencies staff is accessing the internet remotely on the same device that TBIN is accessed then the Agency must have a Data Access Policy in place that explains the Wi-Fi networks that are acceptable to access (secured Wi-Fi networks), examples of how to identify a secured Wi-Fi network, explanation of the impacts of using an unsecure network, and repercussions the user may be subject to by using an unsecure network when using a workstation that accesses TBIN. All users that might use wireless access at any time with the same device that accesses TBIN must sign this policy and the Agency must have record of the signed form. ~~(NEW SECTION)~~

Software Security

Virus Protection: Workstations accessing TBIN shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).

Current Operating System: All workstations that are connected to the same network as workstations accessing TBIN must have a current operating system. A current operating system is any operating system that is being supported and updated continually for security improvements by the software vendor.

Current Browser: All workstations that are connected to the same network as workstations used to access TBIN must have current browsers. A current browser is any browser that is being supported and updated continually for security improvements by the software vendor.

Data Quality

Data Completeness: The Tampa Bay information Network (TBIN) staff will evaluate, monthly, the quality of all TBIN Member Agency data on the completeness of the data entered using a TBIN Report Card. Completeness is the level at which a field has been answered in whole or in its entirety. Measuring completeness ensures client profiles provide an accurate description of the client's situation.

Expectations of Data Completeness: Each month the TBIN staff sends the TBIN Data Completeness Report Card to all Member Agency Administrators. The overall scores identified on the monthly reports indicate the overall completeness and quality of the data answered. A TBIN Member Agency must maintain a grade of 95% or above in TBIN data completeness for all clients served. Member Agency Administrators are given 5 business days to update TBIN Data and bring their report card to 95% or above. A final TBIN Data Completeness Report Card will be ran and set to the Member Agency Administrator and CEO/Executive Director by the 15th of each month.

Commented [AS1]: Kevin's Comment: We just recently made changes to their Policies and procedures on all of this so maybe this Audit Plan should mirror those P&P's

Formatted: Superscript

Data Timeliness

Timeliness of Data: The Tampa Bay Information Network (TBIN) staff monthly, evaluates the quality of all TBIN Member Agency data on the timeliness of the data entered. Entering Client data into TBIN as soon as it is available is important for capturing client information and resources provided to clients. Because TBIN is an open system shared by many other providers it is imperative to enter client data in a timeliness fashion.

Expectations of Data Timeliness: Each month the TBIN staff sends the TBIN Data Timeliness Report Card to all Member Agency Administrators. The overall scores identified on the monthly reports indicate the average time taken to enter/update client information. All TBIN Member Agency client data should be entered in real-time or no later than 24 hours after intake, assessment, program service or entry/exit.

Audit Types

New Member Agency Audit

Prior to establishing access to TBIN for a new Member Agency, the TBIN staff will assess the privacy and security measures in place at the prospective Member Agency as defined in the Privacy and Security sections of this document. TBIN staff will meet with the prospective Member Agency's Executive Director or executive-level designee, to review the Agency's policies and procedures regarding privacy and security prior to granting the requesting Member Agency access to TBIN. This security review shall in no way reduce the Agency's responsibility for information security.

The TBIN Member Agency must be prepared and available on the agreed upon scheduled TBIN New Member Agency Audit. The TBIN New Member Agency Audit will consist of:

1. The TBIN staff conducting the audit will go over the TBIN Audit Form with the Executive Director, its Member Agency Administrator or Executive-level designee. All questions associated with the TBIN Audit Form must be truthfully answered.
2. A walk through of all intake areas, data entry locations, and all other locations that house paper documents containing client information.
3. Any infractions discovered during the TBIN Audit must be corrected by the Requesting Member Agency **within 15 business days** of the Audit.
4. All infractions will be reviewed with Agency staff. A Follow-up Audit is scheduled at this time. The prospective Member Agency will need to complete all corrections documented on the TBIN Audit Form before the Follow-up Audit.

Commented [AS2]: Kevin's comment: I'm not sure this matches the P&P's we just updated

TBIN Staff will provide a copy of the completed TBIN Audit Form to the prospective Agency within 5 business days of completing the audit. A copy of the completed audit form will remain in the TBIN Member Agency's electronic file that TBIN maintains. TBIN Member Agencies may request a copy of any TBIN Audit Form that has been completed. TBIN Member Agency Administrator/Executive-level designee can use the TBIN Audit Form to conduct internal audits at any time they choose, but these cannot be substituted for any TBIN Audit.

Annual Audit

All TBIN Member Agencies must go through a TBIN Annual Audit and must correct all infractions discovered during the audit. This audit shall in no way reduce the Partner Agency's responsibility for information security, which is the full and complete responsibility of the Member Agency.

The TBIN Member Agency must be prepared and available on the agreed upon scheduled TBIN Annual Audit. TBIN staff will use the TBIN Audit Form to perform the TBIN Annual Audit. The TBIN Annual Audit will consist of:

1. The TBIN staff conducting the audit will go over the TBIN Audit Form with the Executive Director, its Member Agency Administrator or Executive-level designee. All questions associated with the TBIN Audit Form must be truthfully answered.
2. A walk through of all intake areas, data entry locations, and all other locations that house paper documents containing client information.
3. Any infractions discovered during the TBIN Audit must be corrected by the TBIN Member Agency **within 15 business days** of the Audit.
4. All infractions will be reviewed with agency staff. A Follow-up Audit is scheduled at this time. The Requesting Member Agency will need to complete all corrections documented on the TBIN Audit Form prior the Follow-up Audit.
5. The TBIN Audit Form will then be signed by both parties.

TBIN Staff will provide a copy of the completed TBIN Audit Form to the audited agency within 5 business days of completing the audit. A copy of the completed audit form will remain in the TBIN Member Agencies electronic file that TBIN maintains. TBIN Member Agencies may request a copy of any TBIN Audit Form that has been completed. TBIN Member Agency Administrator/Executive-level designee can use the TBIN Audit Form to conduct internal audits at any time they choose, but these cannot be substituted for any TBIN Audit.

Follow-up Audit

A Follow-up Audit is an audit that will cover the same requirements as the Annual Audit OR New Member Agency Audit, but it is making sure that the critical ~~changes~~ issues that were ~~needed to be made~~found ~~-~~during the previous Audit have been ~~made~~corrected .

The TBIN Member Agency must be prepared and available on the agreed upon scheduled TBIN Follow-up Audit. TBIN staff will use the TBIN Audit Form to perform the TBIN Follow-up Audit. The TBIN Follow-up Audit will consist of:

1. The TBIN staff conducting the audit will go over the previous TBIN Audit Form and the infractions that were listed, with the Executive Director, its Member Agency Administrator or Executive-level designee. TBIN staff will conduct a new audit with a new TBIN Audit Form. All questions associated with the TBIN Audit Form must be truthfully answered.
2. A walk through of all intake areas, data entry locations, and all other locations that house paper documents containing client information.
3. Any infractions discovered during the TBIN Audit must be corrected by the TBIN Member Agency **within 15 business days** of the Audit.
4. All infractions will be reviewed with Agency staff. A Follow-up Audit is scheduled at this time. The Requesting Member Agency will need to complete all corrections documented on the TBIN Audit Form prior to the Follow-up Audit.
5. The TBIN Audit Form will then be signed by both parties.

TBIN Staff will provide a copy of the completed TBIN Audit Form to the audited agency within 5 business days of completing the audit. A copy of the completed audit form will remain in the TBIN Member Agencies electronic file that TBIN maintains. TBIN Member Agencies may request a copy of any TBIN Audit Form that has been completed. TBIN Member Agency Administrator/Executive-level designee can use the TBIN Audit Form to conduct internal audits at any time they choose, but these cannot be substitute for any TBIN Audit.

Random Audit

TBIN reserves the right to audit any TBIN Member Agency at any time during normal business hours.

The TBIN Member Agency must be prepared and available on the agreed upon scheduled TBIN Random Audit. TBIN staff will use the TBIN Audit Form to perform the TBIN Random Audit. The TBIN Random Audit will consist of:

1. TBIN staff will then conduct an audit with a new TBIN Audit Form. All questions associated with the TBIN Audit Form must be truthfully answered.
2. A walk through of all intake areas, data entry locations, and all other locations that house paper documents containing client information.
3. Any infractions discovered during the TBIN Audit must be corrected by the TBIN Member Agency **within 15 business days** of the Audit.
4. All infractions will be reviewed with the Agency staff. A Follow-up Audit is scheduled at this time.
5. The TBIN Audit Form will then be signed by both parties.

TBIN Staff will provide a copy of the completed TBIN Audit Form to the audited Agency within 5 business days of completing the audit. A copy of the completed audit form will remain in the TBIN Member Agencies electronic file that TBIN maintains. TBIN Member Agencies may request a copy of any TBIN Audit Form that has been completed. TBIN Member Agency Administrator/Executive-level designee can use the TBIN Audit Form to conduct internal audits at any time they choose, but these cannot be substituted for any TBIN Audit.

Participating Agency Responsibilities

It is the responsibility of TBIN Member Agencies to insure compliance with this plan, the TBIN Policies and procedures and all other signed agreements between TBIN and the Member Agency. Each TBIN Member Agency must review and maintain compliance with all TBIN agreements procedures and process. This document serves as the means to measure compliance with privacy, security and HMIS requirements. This document does not serve as the total responsibility of the TBIN Member Agency. It only serves as a guideline and measure of compliance that each member agency must abide by, but is not limited to.

Infractions

Any items that are not implemented or maintained by the TBIN Audit Form are considered infractions. Any infraction discovered during any TBIN Audit must be corrected within 15 business days of the audit. Each section of the TBIN Audit Form consists of points that can be earned if the section has been implemented or partially implemented. There are a total of 50 points that can be earned during a TBIN Audit. Letter grades are associated with the points earned. The letter grade earned during a TBIN Audit will determine if a Follow-up Audit is necessary and the level of severity the Member Agency is not in compliance. The letter grade tiers are listed below:

i. **Grades of A - B:** TBIN Member Agency's that earn a grand total of 40 to 50 points must correct all infractions within 15 business days of the audit date.
ii. **Grades of C - D:** TBIN Member Agency's that earn a grand total of 20 to 39 points must correct all infractions within 15 business days of the audit date and a follow-up audit must be completed within 20 business days of the completed audit.
iii. **Grade of F:** TBIN Member Agency's that earn less than 19 points must correct all infractions within 15 business days or develop an action plan within 15 business days of the completed audit, that will correct each item as soon as possible. The action plan must contain the infraction items, steps to correct each item, and an expected completion date of each item. The TBIN Member Agency must email the action plan within 15 business days of the completed audit to the TBIN Help Desk at www.tbin.zendesk.com. Failure to comply could result in the TBIN Member Agency loosing access and the access of all of their staff to the TBIN system. Any change in access will be reported to local funding entities, the Data and System Performance Committee, and the HLB.

Commented [AS3]: Kevin's comments: This does not really match the P&P's that we just updated. I don't think 211 has played an active role in this process as well. They have provided and prepared the reports but were not historically doing follow-up. This function sort of fell on the System Data Performance Committee in it's various names but with no real authority.

Reporting

All completed TBIN Audit Forms will be reviewed by the Data and Systems Performance Committee on a quarterly basis. At any time TBIN reserves the right to report any TBIN Member Agency's completed TBIN Audit Form to the Data and System Performance Committee for their review. TBIN and the HLB can revoke access to TBIN for any TBIN Member Agency, its employees, volunteers, affiliates, contractors, and associates for noncompliance of any of the items not completed in this TBIN Audit Plan. TBIN and the HLB can also deny access to any prospective Member Agency that does not comply with this TBIN Audit Plan or any item in the TBIN Audit Form before gaining access to TBIN.