TUSCOLA BEHAVIORAL HEALTH SYSTEMS
COMPLIANCE POLICIES

TABLE OF CONTENTS

COMPLIANCE

Duties of the Compliance Officer & Compliance Committee Members X-001-001
Acquisition & Maintenance of Third Party Payer Publications X-001-002
Internal Reporting X-001-003
Internal Non-Retaliation & Discipline X-001-004
Internal Investigation & Confidentiality X-001-005
Document Retention X-001-006
Internal Government/Third Party Payer Investigation X-001-007
Compliance Department Training Updates X-001-008
Accreditation Maintenance X-001-009
Licensing Maintenance X-001-010

EDUCATION

Clinical Documentation X-002-001
Written Plan of Service & Person-Centered Planning X-002-002
Medical Necessity X-002-003
Range of Services X-002-004
Medicaid Eligibility X-002-005
Cost Reporting X-002-006
Marketing & Public Relations X-002-007
Collection of Co-Payments & Deductibles X-002-008
Review Procedures for Contractual/Ownership Arrangements X-002-009
Claim Preparation & Submission X-002-010

HIPAA PRIVACY

Complaints from Individuals Served X-003-001
Safeguarding Faxes X-003-002
Minimum Necessary/Need to Know Protocols for Routine Disclosures
to Medicaid & Other Health Plans X-003-003
Uses & Disclosures Restricted to – Minimum Necessary Information X-003-004
Notice of Privacy Practices X-003-005
Personal Representatives X-003-006
Reasonable Safeguards X-003-007
Individuals Right to Request Access or Amendment to Records X-003-008
Rights of Individuals-Restrictions on Use of Protected Health Information X-003-009
Routine Uses & Disclosures X-003-010
Uses & Disclosures Involving Authorizations X-003-011
Uses & Disclosures Involving Special Circumstances X-003-012
Social Security Numbers X-003-013
Breach Notification X-003-014

HIPAA SECURITY

Business Associate Agreement X-004-001
Computer Access X-004-002
Data Back-Up X-004-003
Designation & Responsibilities of Security Officer X-004-004
Disaster Recovery Contingency Plan X-004-005
Electronic Device Use X-004-006
E-Mailing of Protected Health Information X-004-007
Emergency Mode Operations Plan X-004-008
Firewalls X-004-009
General Rules to Safeguard TBHS Computer Network X-004-010
Monitoring X-004-011
Physical Security X-004-012
Remote Access X-004-013
Reporting of Security Incidents-Mitigation of Harm X-004-014
Sanctions X-004-015
Change of Employment Status X-004-016
User Names & Passwords X-004-017
Virus & Other Malicious Software Management X-004-018
Wireless Access X-004-019
Workforce Clearance X-004-020
Electronic Signatures X-004-021

Tuscola Behavioral Health Systems (also known as Tuscola County Community Mental Health Authority) Compliance Policies listed above, have been reviewed and approved by the Chief Executive Officer.

Review Date: 9/19/22

Approved By: Beals

Policy Section	Compliance	Policy Number	X-001-001
Subject	Duties of the Compliance Officer & Compliance Committee Members	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that the Compliance Officer shall serve as the focal point for TBHS' compliance activities.

PURPOSE

The purpose of this policy is to identify the Compliance Officer and Compliance Committee processes.

APPLICATION

This policy shall be applicable to staff of the TBHS Compliance Department.

DEFINITIONS

Not applicable.

PROCEDURES

The Compliance Officer's primary responsibilities include the following:

- Overseeing the daily operations of the Program
- Reporting to the CEO on compliance matters
- Recommending revisions to the program and policies, as necessary
- Coordinating and participating in education
- Investigating and acting on reported compliance related concerns
- Overseeing that TBHS acquires and maintains applicable third-party publications
- Overseeing that the monitoring and education plan is being followed. The Compliance Officer shall actively work to ensure that the monitoring and education plan is followed by TBHS
- Reporting to MSHN any suspected or known Medicaid fraud or abuse

The Compliance Committee members' primary responsibilities shall include the following:

- Meeting on sensitive compliance issues requiring decisions regarding potential corrective action
- Assisting the Compliance Officer in monitoring, revising, and updating the Compliance Program and policies, as necessary
- Keeping apprised of changes in regulations, payer requirements, etc. that affect TBHS
- Recommending the development and implementation of policies to address risk areas
- Participating in the educational and monitoring process

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
10/06/2014
10/06/2015
09/20/2022

Policy Section	Compliance	Policy Number	X-001-002
Subject	Acquisition & Maintenance of Third Party Payer Publications	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Teresa Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to acquire and maintain applicable third party payer publications and maintain a library of all manuals, bulletins, contracts, and other relevant publications published by the major third party payers to which TBHS submits claims and/or cost reports for community mental health and related services.

PURPOSE

The TBHS Compliance Officer, or his/her designee, will be responsible for overseeing that TBHS has a copy of applicable manuals, bulletins, contracts, and other relevant publications published by the major third party payers to which TBHS submits claims and/or cost reports for services and that TBHS is receiving all such materials.

APPLICATION

This policy shall be applicable to staff of the TBHS Compliance Department.

DEFINITIONS

Not applicable.

PROCEDURES

TBHS will place particular emphasis with regard to acquiring and appropriately maintaining all Medicaid manuals and bulletins applicable to community mental health services providers such as the Michigan Medicaid Community Mental Health Services Manual. The TBHS Compliance Officer shall ensure that the finance department has a complete Michigan Medicaid Community Mental Health Services Manual and the Michigan Department of Health and Human Services Program Contract with attachments.

The Compliance Officer, or his/her designee and one member of the finance department, with approval of their supervisor, shall also be responsible for reviewing applicable publications, bulletins, and/or manuals when received by TBHS to determine if such information should be disseminated to relevant employees and subcontractors. If pertinent information is gleaned from these publications, the Compliance Officer, or his/her designee, shall have an established internal distribution system in place so that relevant materials may be distributed to TBHS staff and subcontractors whose job duties/functions are impacted by the information.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
04/06/2010
10/06/2014
10/06/2015
09/20/2022

Policy Section	Compliance	Policy Number	X-001-003
Subject	Internal Reporting	Issue Date	04/06/2010
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that upon receipt of a compliance incident report, the Compliance Officer shall handle such report in accordance with TBHS' procedure for the investigation of perceived violations.

PURPOSE

The purpose of this policy is for employees and subcontractors to have a process for reporting perceived violations of the compliance program and applicable healthcare laws, its incorporated policies and/or applicable Federal, state and third party payer rules to the Compliance Officer pursuant to the procedure set forth below.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Reporting:

Employees and subcontractors may report any compliance-related concerns to the TBHS Compliance Officer by any of the following methods:

1. Filling out a copy of the TBHS Compliance Incident Report Form (copies of this form can be found on the G: drive in the TBHS Approved Forms folder) and placing such form in a sealed envelope marked "CONFIDENTIAL" and addressing the envelope to the Compliance Officer;
2. Directly speaking to the Compliance Officer in person and making such report verbally;
3. Calling the TBHS compliance hotline. The hotline number is (989) 672-3145. It is password protected and rings to a dedicated line;
4. MSHN Compliance Hotline: 1-844-793-1288;
5. MDHHS Medicaid Fraud Hotline: 1-855-MI-FRAUD (643-7283) or online at https://www.michigan.gov/mdhhs/0,5885,7-339-71551_2945_42542_42543_42546_42551-220056--,00.html; or
6. HHS/OIG Hotline: 1-800-HHS-TIPS (447-8477) or online at https://oig.hhs.gov/fraud/report-fraud/.

All reports of compliance-related concerns will be taken seriously, and clarification or advice will be handled as appropriate. It is TBHS' intent to fully comply with the Michigan Whistleblower's Protection Act, the Michigan Medicaid False Claims Act, and Federal Civil False Claims Act.

The Compliance Officer shall complete a report of findings within five (5) business days of completion of the investigation. This timeframe shall be considered a prompt response to any detected offense, or for any development of corrective action determined to be a part of the investigation.

Human Resource issues should be directed to the Human Resources Supervisor and not the Compliance Officer.

RELATED FORMS & MATERIALS

Compliance Incident Report form.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
04/06/2010
08/05/2011
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/20/2022

Policy Section	Compliance	Policy Number	X-001-004
Subject	Internal Non-Retaliation and Discipline	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that no employee who makes a report of alleged wrongdoing regarding substantiated claims, as determined by TBHS, of wrongdoing in violation of the compliance program or its incorporated policies in good faith will be subjected to reprisal, harassment, retribution, discipline or discrimination by TBHS or any of its employees or agents based on having made the report.

PURPOSE

The purpose of this policy is for employees to use the compliance program as a guide to enhance compliance with all applicable federal, state, and third party payer laws, rules, regulations and policies. Any TBHS employee or agent who engages in any such reprisal, harassment, retribution, discipline or discrimination against a good faith reporter may be subject to disciplinary action as deemed appropriate by TBHS.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

The Michigan Whistleblower's Protection Act provides protection to employees who report a violation or suspected violation of state, local or federal law. The Michigan Medicaid False Claims Act also provides protection for employees who initiate, assist or participate in a proceeding or court action under this law or who cooperate or assist with investigations conducted under this law.

The Fraud Enforcement and Recovery Act of 2009 (FERA) expands the federal-level Civil False Claims Act and now provides protection that: "any employee, contractor, or agent shall be entitled to all relief necessary to make that employee, contractor, or agent whole, if that employee, contractor, or agent is discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms and conditions of employment because of lawful acts done by the employee, contractor, or agent on behalf of the employee, contractor, or agent or associated others in furtherance of other efforts to stop one or more violations."

However, an employee will be subject to disciplinary action if TBHS concludes that the employee knew or should have known that the reporting of wrongdoing was fabricated, not based on true facts or made in bad faith or that the report was distorted, exaggerated or minimized to either injure someone else or to protect him/herself or others.

In order to effectively enforce the compliance program and incorporated policies, the TBHS Compliance Officer may recommend to the CEO and Human Resources Supervisor that disciplinary action be taken against an employee for failure to comply with the compliance program and/or the incorporated policies. However, the CEO and Human Resources Supervisor will maintain authority over employee discipline issues.

Physician Employees

With regard to physician employees of TBHS, the proposed disciplinary action may include, at the sole discretion of TBHS, such sanctions ranging from, but not limited to: (1) the employee's personal payment of the cost of his/her re-education; (2) the cost of an audit to monitor his/her compliance; (3) the cost of services TBHS is unable to bill due to lack of compliance; (4) suspension; and/or (5) termination.

Non-Physician Employees

With regard to non-physician employees of TBHS, the proposed disciplinary action may include, at the sole discretion of TBHS, such sanctions ranging from, but not limited to: (1) oral counseling; (2) an official reprimand; (3) suspension; and/or (4) termination.

TBHS remains an at-will employer who may discharge any employee with or without notice and with or without cause. Nothing in this policy alters or shall be construed to alter the at-will employment of TBHS' employees.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Public Law 111-21: Fraud Enforcement and Recovery Act of 2009.

Michigan Compiled Laws Act 469 of 1980: The Whistleblower's Protection Act.

Revision Dates:
04/06/2010
05/17/2012
10/06/2014
10/06/2015
09/20/2022

Policy Section	Compliance	Policy Number	X-001-005
Subject	Internal Investigation & Confidentiality	Issue Date	04/06/2010
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that the Compliance Officer shall investigate reported compliance-related concerns.

PURPOSE

The purpose of this policy is to delineate investigation procedures when a compliance-related concern is reported.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Compliance Committee: The primary purpose of the Compliance Committee is to provide oversight and guidance to the Compliance Program with respect to compliance with laws, regulations and policies applicable to TBHS Programs, direct or contracted.

PROCEDURES

Upon receipt of a compliance incident report form, a call to the compliance hotline, or otherwise learning of a compliance concern, the Compliance Officer shall take responsibility for the investigation and shall contact legal counsel, for further direction if deemed necessary, if in the judgment of the Compliance Officer the matter merits investigation (e.g., not a human resources issue).

Within five business days of receiving the complaint, the Compliance Officer shall provide a written acknowledgment of receipt to the individual making the complaint (if known).

After receiving direction from legal counsel, if applicable, the Compliance Officer shall undertake an investigation of the reported concern by reviewing necessary information as well as conducting any necessary interviews with employees or other individuals as necessary. In those circumstances in which the reporting employee has provided his/her name, the Compliance Officer shall interview such employee.

If it has been determined that the matter requires further investigation, the Compliance Officer shall take the necessary steps to assure that documents or other evidence are not altered or destroyed through the following means, as applicable:

- Suspending normal record/document destruction procedures;
- Taking control of the files of individuals suspected of wrongdoing;

- Limiting access of files, computers and other sources of documents by individuals suspected of wrongdoing; and/or
- Taking additional action as necessary to ensure the integrity of the investigation that could include temporary suspension, or temporary re-assignment of duties, of involved individuals.

The Compliance Officer shall keep all investigation materials (including interview notes and reports, etc.) in a confidential folder marked attorney/client privileged. This information should not be shared with others. Upon completion of this process, the Compliance Officer shall contact legal counsel and provide a summary of the investigation. If it is determined that the matter does not constitute a violation of any applicable laws or regulations and warrants no further action, the issue will be closed following the appropriate documentation and reporting by the Compliance Officer.

If it is determined that the matter does not constitute a violation of any applicable laws or regulations, but does identify an area for improvement or raises concern for potential future violations, the matter will be referred to the Compliance Committee for discussion.

If the outcome of an internal investigation is substantiation of the reported violation, a corrective action plan will be developed. Corrective action plans developed by TBHS must be submitted to MSHN within 30 days of completion.

Investigations involving MSHN

If the MSHN Compliance Officer has determined that reporting to a government agency (e.g., Centers for Medicare and Medicaid Services (CMS), Office of Inspector General (OIG), and Department of Justice (DOJ)) or a third party may be appropriate, the TBHS Compliance Officer will be informed that MSHN will be reporting the issue to the government agency. The TBHS Compliance Officer will cease investigation of the issue until the MSHN Compliance Officer informs the TBHS Compliance Officer to proceed.

If MSHN does not receive confirmation from MDHHS Office of Health Services Inspector General (OHSIG) or if OHSIG instructs MSHN to not conduct any further investigation, MSHN shall document the OHSIG communication and follow up with the OHSIG within thirty (30) days to obtain an update on the case. The TBHS Compliance Officer will not take any action during this time.

Reporting

The Compliance Officer reports to the CEO. In the absence of a Compliance Officer, the CEO shall serve as the Compliance Officer. In the event there is a compliance allegation or complaint relating directly to the CEO, the Compliance Officer shall automatically report the matter directly to the Chair of the TBHS Board of Directors. If the CEO is serving as the Compliance Officer and an allegation or complaint relates to the CEO, the complaint should be made to the Chief Operating Officer (COO) who will notify legal counsel. Legal counsel would then work directly with the Chair of the TBHS Board of Directors.

Depending on the results of the investigation and nature of the issue, the TBHS Compliance Officer may call a Compliance Committee Meeting (which may require the presence of legal counsel depending on the nature of the issues uncovered in the attorney/client privileged investigation) to discuss the results and any corrective action that should be taken. The Compliance Committee shall in turn make recommendations to the CEO regarding any corrective action that should be taken.

TBHS shall report quarterly to the PIHP the number of complaints of fraud, waste, abuse, and other compliance related issues that warranted preliminary investigation. The following information shall be forwarded to the PIHP in compliance with PIHP and CMHSP reporting requirements:

- Tips/grievances received
- Data mining and analysis of paid claims, including audits performed based on the results
- Audits performed
- Overpayments collected
- Identification and investigation of fraud, waste and abuse
- Corrective action plans implemented
- Provider dis-enrollments
- Contract terminations

Confidentiality

With the exception of disclosure to authorized individuals, or as required by law, the Compliance Officer will make good faith efforts to maintain the confidentiality of reporters of compliance-related concerns. Callers to the compliance hotline will be identified using a caller identification number on the hotline reporting form. The Compliance Officer or any other staff, upon assignment to the TBHS Compliance Office, should sign a confidentiality non-disclosure agreement barring disclosure of reported compliance-related issues to unauthorized individuals.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
10/06/2014
10/06/2015
11/30/2016
10/16/2019
10/14/2020
09/20/2022

Policy Section	Compliance	Policy Number	X-001-006
Subject	Document Retention	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Dawn Birks
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that employees are required to use good faith efforts to adhere to TBHS document retention procedures, including retention of finance records.

PURPOSE

TBHS employees are required to use good faith efforts to adhere to TBHS document retention procedures, including retention of finance records.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Documents:

Documents must be maintained in English and in a legible manner. Documents covered under this policy shall include all billing, compliance and related documents including, but not limited to, the following:

1. Cost reports
2. Claim forms submitted to Medicare, Medicaid and other third party payers and claim forms submitted for internal cost reporting tracking purposes
3. Supporting documentation for the cost reports and claim forms
4. Pertinent correspondence related to cost reports, claim forms or other billing matters
5. Medical/Clinical records
6. Documentation of TBHS' compliance educational efforts
7. Incident Reports and Compliance Hotline Reports generated pursuant to the compliance program
8. Service activity logs
9. Remittance advices, as applicable
10. Prior authorization requests and approvals for services and supplies (including managed care authorizations)
11. Verifications of medical necessity and the provider's usual and customary charge for non-covered services
12. Records of third-party payment
13. Purchase invoices for items offered or supplied to individuals served

Document Retention Period:

All documents covered under this policy should be properly maintained and retained by TBHS, or another party designated by TBHS, for a period of no less than seven (7) years unless otherwise stipulated by law, from the date of service or termination of service for any reason, the date of the cost report or the document inception date. Original medical records shall be maintained in full accordance with Michigan law. Documents retained under this policy shall be maintained in accordance with TBHS' confidentiality procedures, as applicable.

The HIPAA Privacy Rule states that health information regarding a person who has been deceased for more than 50 years is excluded from the definition of PHI. State laws would still take precedent, as applicable.

Document Destruction:

Confidential documents destroyed under this policy shall be disposed of in a manner that will not compromise their confidentiality.

Reporting Improper Destruction of Documents

No employee or other person shall destroy or alter any document maintained by TBHS, or maintained by another party for TBHS, in anticipation of a request for those documents from any governmental agency or court. If any TBHS employee believes that such conduct has occurred or may occur, she/he shall contact the Compliance Officer immediately via the internal reporting mechanisms.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Michigan Medicaid Community Provider Manual
MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement, Part 1 Section 13

Revision Date:
04/06/2010
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/17/2018
09/20/2022

Policy Section	Compliance	Policy Number	X-001-007
Subject	Internal Government/Third Party Payer Investigation	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Susan Beals
		Page	1 of 5

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that if any employee receives an inquiry, subpoena, or other legal document from any governmental agency or third party payer regarding or relating in any way to TBHS' operations, whether at home or in the workplace, TBHS requests that the TBHS employee notify the TBHS Compliance Officer and/or TBHS' Chief Executive Officer or Chief Operating Officer immediately.

PURPOSE

The purpose of this policy is to allow TBHS to effectively monitor compliance with the government's/third party payer's investigation and to assure that the information conveyed to the government/third party payer is accurate, appropriate and not subject to a legal or other privilege.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Notice to the Compliance Officer

If a TBHS employee is visited at home or in the community by a governmental agent concerning or relating in any way to TBHS, the TBHS employee is legally entitled to ask the agent to return, at his/her option, and should immediately contact the TBHS Compliance Officer and/or TBHS' Chief Executive Officer or Chief Operating Officer to discuss the matter. TBHS may arrange for its legal counsel to accompany the TBHS employee to any government interview in order to protect the legitimate business interests of TBHS. At his/her option, the TBHS employee may also choose to retain his/her own lawyer in order to protect his/her own interests. Providing false or inaccurate information to a government agent might constitute a criminal offense. Moreover, providing false, inaccurate or privileged information to a third party may have serious economic and/or legal consequences for TBHS and could result in disciplinary action against the TBHS employee.

TBHS expects that its employees will notify the TBHS Compliance Officer and/or TBHS' Chief Executive Officer or Chief Operating Officer if the employee believes that the government has initiated an investigation with regard to TBHS or any party affiliated with TBHS. In the event that the TBHS employee is unsure as to whether an investigation has been undertaken, the employee should consult with the Compliance Officer and/or the TBHS Chief Executive Officer or Chief Operating Officer.

Initial Contact

Upon initial contact with the agent/auditor/investigator (whether in-person or over the telephone), TBHS employees should explain that TBHS has a specific policy to follow in such circumstances and that TBHS requires each employee to obtain information regarding the specific nature of the audit, inquiry and/or investigation, including, but not limited to:

1. The full name, title, telephone number and address of the auditor/investigator. [If contact is in-person, the employee should ask for identification and record the information from the identifying source];

2. The name of the agency or authority that is conducting the audit/investigation;

3. The full name, title, telephone number and address of any other auditor/investigator or attorney(s) involved in the audit/investigation;

4. The general subject matter about which the auditor/investigator wishes to question the employee and how long it will take;

5. Whether the inquiry is civil or criminal; and

6. The legal authority for the investigation and examination of records (e.g., a subpoena, search warrant, civil investigative demands).

Subpoenas

Per TBHS Medical Records Procedure; "Subpoenas;" the following protocol shall be adhered to:

1. All orders or subpoenas from a court of record, i.e., Probate/Family Court, District Court, Circuit Court, Court of Claims, or a subpoena of the legislature must be honored, unless the information is privileged by law. (A court of record does not include state administrative agency, Bureau of Worker's Compensation, or a record copy service).

2. Subpoenas should be accompanied by an Authorization to Release/Exchange Information, if issued by an attorney. Subpoenas issued by a court of law would be considered a Court Order. Refer to the Clinical Search Warrants Procedure for further information.

3. Although not typically permitted, TBHS has allowed subpoenas for records or documentation to be received via email during the COVID-19 pandemic. Upon receipt of a subpoena in this manner, the subpoena is to be routed for processing.

4. Upon receipt of a subpoena to produce information, the Medical Records staff shall enter the requested information on the Medical Records Disclosure Tracking Log.

5. If no Authorization to Release/Exchange Information accompanies the subpoena, the Medical Records staff shall verbally request an Authorization to Release/Exchange Information from the party/entity who issued the subpoena. Documentation of the request shall be attached to the initial request and scanned into the individual's record.

6. If no Authorization to Release/Exchange Information is provided by the issuer of the subpoena the Medical Records Specialist will respond in writing, explaining TBHS cannot comply with the subpoena. The explanation must indicate the reason for the denial of release, i.e. no required Authorization to Release/Exchange Information accompanying subpoena, the subpoena was not served in the required timeframe, invalid subpoena, etc. The explanation must reach the issuer prior to the due date.

7. Medical Records staff are to confirm the validity of the subpoena by reviewing the following items:

    a. Must be entitled in the name of the people of the state of Michigan;
    b. Must have the name of the court in which the matter is pending (typed or printed);
    c. Must state the time and place of the trial, hearing, deposition and/or where the documents are to be delivered;
    d. Must state whether documents are to be produced, a person is to provide testimony, or both;
    e. Must state the title of the action in which the person is expected to provide testimony and/or produce documents;
    f. Must state the file number assigned the case by the court;
    g. Must state that the failure to obey the commands of the subpoena or reasonable direction of the signer as to the time and place to appear and/or produce documents, may subject the person to whom it is directed to penalties;
    h. Must be signed by an authorized signature, i.e. the name of the judge, a court clerk or an attorney representing a party to the action; and
    i. Must be served at least two calendar days before the witness is to attend, unless otherwise ordered by the court; for discovery of medical information, TBHS has 14 days to respond to the request, unless the court has extended or shortened the time frame on motion for good cause.

Should any questions arise regarding the validity of the subpoena, Medical Records staff are to contact the Health Information Specialist for further guidance.

8. A Record of Disclosure shall be completed in the electronic health record (EMMIT) of the individual served each time information is released externally from their record.

9. Once the requested information has been released, the Medicals Records Disclosure Tracking Log shall be updated to indicate the date of release.

On-Site Inquiries

After obtaining the information in the paragraph above entitled "Initial Contact", if the agent/auditor/investigator is on TBHS premises, the employee may, at his/her option, instruct the agent/auditor/investigator that the employee wishes to consult with TBHS' legal counsel prior to being interviewed or questioned and that the employee or TBHS legal counsel will call the agent/auditor/investigator with regard to how TBHS wishes to proceed. While TBHS wishes to cooperate fully with all reasonable demands made in a government and/or third party payer audit and/or investigation, it must do so in such a manner as to minimize the disruption to TBHS' normal business activities and to protect the legal rights of TBHS and its employees. It is important to understand that

certain information sought by the agent/auditor/investigator, and/or its receipt, may be privileged or unauthorized and therefore should be reviewed by TBHS counsel prior to its release to the agent/auditor/investigator. Thus, while TBHS appreciates that the presence of an agent/auditor/investigator may be unnerving, TBHS strongly encourages its employees not to permit the agent/auditor/investigator to threaten or cajole the employee to follow any other course of action.

A memorandum summarizing the information obtained from the agent/auditor/ investigator should be conveyed to the TBHS Compliance Officer as soon as practicable and should include the above-described information from the initial contact as well as any other information and/or observations that the employee can recall from his or her contact with the agent/auditor/investigator.

Off-Site Inquiries

After obtaining the information in the paragraph above entitled "Initial Contact", if the agent/auditor/investigator is not on TBHS premises (e.g., contact is made at the employee's home or in the community), the employee has the option of speaking with the agent/auditor/investigator, requesting to speak with the agent/auditor/investigator at a more convenient time (e.g., during normal business hours on TBHS premises---after having confirmed the time and place with the TBHS Compliance Officer) or politely declining to speak with the agent/auditor/investigator. In addition, the employee has the right to have legal counsel present during any interview. The employee may have his or her own legal counsel present and/or request TBHS to have its counsel present at no cost to the employee. The employee should be aware that TBHS counsel's first priority is to protect the lawful business interests of its client, TBHS, not the TBHS employee, and therefore, the TBHS employee has the right to retain his/her own counsel in order to protect his/her own interests. If the employee has any doubts about his or her rights or how to handle the situation, the employee should not hesitate to contact his or her attorney or the TBHS Compliance Officer.

A memorandum summarizing the information obtained from the agent/auditor/investigator should be conveyed to the TBHS Compliance Officer as soon as practicable and should include the above-described information from the initial contact as well as any other information and/or observations that the employee can recall from his or her contact with the agent/auditor/investigator.

During the Interview

During the interview, TBHS employees should take care not to show or provide any TBHS documents or copies of TBHS documents to the agent/auditor/investigator without prior authorization from the TBHS CEO or his/her designee as such documents may be privileged. Moreover, TBHS employees should maintain a separate copy of every document provided to the agent/auditor/investigator and a list of every document shown to the agent/auditor/investigator.

If unaccompanied by counsel during the interview, TBHS employees should draft detailed memorandums summarizing the information given to, and obtained from, the agent/auditor/investigator. Such memorandums should be conveyed to the TBHS CEO as soon as practicable and should include the above-described information from the initial contact as well as any other information and/or observations that the employees can recall from their contact with the agent/auditor/investigator.

Interference/Obstruction

TBHS has a firm policy against interfering and/or obstructing in audits and/or investigations. As such, TBHS employees **shall under no circumstances**:

1. Destroy or alter any TBHS document or record in anticipation of a request or demand of the document or record by a government agency or court;

2. Make false or misleading statements or lie to any government agent or investigator; and/or

3. Attempt to persuade any other TBHS employee, or any other person, to provide false or misleading information to a government audit or investigation or to refuse to cooperate with a government audit or investigation.

Notification to MSHN & Other Parties

MSHN shall be informed, in writing within three business days, of any material notice to, inquiry from, or investigation by any federal, state or local human services, fiscal, regulatory, investigatory (excluding Recipient Rights related to non-PIHP activities), prosecutor, judicial, or law enforcement agency or protection and/or advocacy organization regarding the rights, safety, or care of a recipient of Medicaid services. The MSHN CEO will also be notified of any subsequent findings, recommendations, and results of such notices, inquiries or investigations.

Written notification will also be provided as required by MDHHS, OIG, etc.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Provider Network Procedures Manual, Medical Records, Chapter: Medical Records, Subject: Subpoenas.

Revision Date:
04/06/2010
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/17/2018
10/16/2019
09/02/2021
09/20/2022

Policy Section	Compliance	Policy Number	X-001-008
Subject	Compliance Department Training Updates	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to ensure that the Compliance Department and Compliance Officer receive and maintain periodic education on all relevant areas of corporate compliance to ensure competence.

PURPOSE

The purpose of this policy is to establish a process whereby the Compliance Department and the Compliance Officer receive (through appropriately sanctioned sources-see procedures), the appropriate education and training to subsequently provide the appropriate oversight and guidance related to current applicable local, state and federal laws, rules, regulations and requirements.

APPLICATION

This policy shall be applicable to staff of the TBHS Compliance Department.

DEFINITIONS

Not applicable.

PROCEDURES

Training of the Compliance Department

1. The TBHS Corporate Compliance Department shall obtain and maintain pertinent contemporary compliance information. Sources for this information shall include:

   a. TBHS membership in national and state organization(s) recognized as leaders in behavioral healthcare issues, including but not limited to, The National Council for Behavioral Health (National Council) and Community Mental Health Association of Michigan (CMHA).

   b. Ongoing environmental scan of state and federal offices, including, but not limited to, the Michigan Department of Health and Human Services (MDHHS), the Michigan Attorney General, The United States Department of Health and Human Services (DHHS), including the Centers for Medicare and Medicaid Services (CMS) and the United States Office of the Inspector General (OIG), and all other state and federal offices as applicable. The Compliance Department shall not interpret any statutes or laws. The attorney retained for purposes of compliance law interpretation shall perform this function.

   c. Regional compliance meetings as needed, activity and communication, which shall be the forum for sharing all relevant compliance updates, requirements and information.

d. The law firm procured for regional compliance efforts will be utilized, as appropriate, to provide updates on information and issues pertaining to corporate compliance and behavioral healthcare.

e. Education shall occur annually through conference attendance, trainings, web-based learning, listserves, meetings, etc.

2. The Compliance Department shall annually review the Corporate Compliance Program Monitoring and Education Plan.

a. Based on any changes in compliance program requirements obtained from any of the aforementioned sources in part I. of this policy, the compliance department shall review the changes and determine a plan for integrating the changes. Any recommended changes shall be approved by the TBHS Chief Executive Officer.

b. In turn, all changes shall be reflected in updated trainings of TBHS staff.

c. The TBHS Training Department shall be provided with an updated Corporate Compliance training packet any time any such update has been made.

d. As appropriate, the TBHS Board of Directors will be provided education related to the Compliance program and applicable laws and regulations.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

42 CFR 422.503 (b) (4) (vi) (c)

Revision Dates:
04/06/2010
06/01/2012
11/19/2013
10/06/2014
10/06/2015
09/17/2018
10/16/2019
09/20/2022

Policy Section	Compliance	Policy Number	X-001-009
Subject	Accreditation Maintenance	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to be committed to the accreditation process through compliance with the internationally recognized standards of the Commission on Accreditation of Rehabilitation Facilities (CARF) International.

PURPOSE

The purpose of this policy is to ensure that TBHS continually provides high quality treatment and care and receives and maintains accreditation by an industry-recognized accrediting organization.

APPLICATION

This policy shall be applicable to staff of all direct operated TBHS Programs

DEFINITIONS

CARF International: The Commission on Accreditation of Rehabilitation Facilities

PROCEDURES

Accreditation Maintenance:

1. TBHS Administration will assure that TBHS has the most current Behavioral Health Standards Manual issued by CARF, and any other applicable manual under which TBHS may be reviewed.

2. TBHS Administration shall be responsible for maintaining the process of CARF standards review. As appropriate, the Leadership and Clinical Management Teams will be utilized for feedback in areas of standard adherence that pertain to administration or general program standards.

3. Accredited programs/departments shall be responsible for compliance with standards pertaining to behavioral health care program standards, specific population designation standards and employment and community services standards.

4. CARF will audit/review TBHS on a re-occurring basis. Prior to and during reviews, the Quality Systems and Compliance Supervisor will ensure that all programs, supervisors, and employees are up to date on applicable CARF standards. This will be ensured by partnering with program supervisors annually, if applicable, for CARF standard changes and suggesting ways to meet new standards.

5. TBHS Administration shall also follow through with any CARF-required plans of correction or improvement as indicated and in conjunction with the appropriate committee or department.

6. Annually, TBHS Administration shall review CARF changes in standards and keep TBHS Leadership up to date on any changes that need to occur.

7. TBHS Leadership be kept up to date on all reports of progress toward correction and status of annual reports submitted to CARF as appropriate.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
11/30/2016
10/14/2020
09/20/2022

Policy Section	Compliance	Policy Number	X-001-010
Subject	Licensing Maintenance	Issue Date	11/06/2009
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to be committed to the licensing standards established by the State of Michigan, Department of Health Human Services and Office of Children and Adult Licensing.

PURPOSE

The purpose of this policy is to ensure that TBHS continually provides high quality care within their direct operated residential homes.

APPLICATION

This policy shall be applicable to staff of TBHS direct operated residential homes.

DEFINITIONS

Not applicable.

PROCEDURES

1. Residential Services Supervisors will monitor the residential homes on an ongoing basis against the licensing standards.
2. Residential Services Supervisors will incorporate changes to the licensing standards into the home operating procedures, when applicable.
3. Residential Services Supervisors will participate in licensing reviews conducted by the Bureau of Children and Adult Licensing and will address in a timely manner any identified findings.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

State of Michigan, Department of Health and Human Services, Department of Licensing and Regulatory Affairs – Bureau of Community & Health Systems Licensing Rules for Adult Foster Care, Family Home and Group Home.

Revision Dates:
10/06/2014
10/06/2015
10/08/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-001
Subject	Clinical Documentation	Issue Date	04/06/2010
		Revision Date	09/20/2022
		Approved By	Sharon Betts
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to use reasonably good faith efforts to ensure that the clinical records of individuals served contain complete, accurate and legible documentation. Moreover, that such records comply with all government, third party payer and accreditation organization requirements regarding clinical documentation of individuals served.

PURPOSE

The purpose of this policy is to ensure that all information documented in the clinical record should be truthful, valid, and accurate.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

TBHS employees, independent contractors and subcontractors are responsible for using reasonably good faith efforts to comply with this policy. TBHS will work in coordination with its subcontractors to effectuate this policy. Clinical records of individuals served, per Clinical Policy IV-003-001; "Medical Record Documentation," should contain, at a minimum, the following information, as applicable:

1. Demographic / Identifying Information
2. Treatment Documentation
3. Medication or other Adjunct Medical Service Documentation
4. Financial Documentation

Please refer to the "Medical Records Requirements" attachment on Clinical Policy IV-003-001 for specific information regarding the above minimum requirements.

Employees should immediately report any violations of this policy to the Compliance Officer through the internal reporting mechanisms.

Each individual's health record should indicate the specific findings or results of diagnostic or therapeutic procedures. Abbreviations used must be standard and widely accepted health care terminology.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Michigan Medicaid Provider Manual
Michigan Mental Health Code- MCLA Section 330.1141
Clinical Policy, IV-003-001; "Medical Record Documentation"
CARF Behavioral Health Standards Manual 2022, Section 2.G.4, a-v

Revision Date:
04/06/2010
08/05/2011
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/17/2018
10/16/2019
10/14/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-002
Subject	Written Plan of Service & Person-Centered Planning	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that staff uses the Person-Centered Planning (PCP) process in developing a written individual plan of service for an individual served and that good faith efforts are used to fully document this process. Further, in each PCP written plan of service, the individual's dreams, desires and goals will be identified, addressed and documented as well as the individual's strengths, cultural background and safety and health issues.

PURPOSE

The purpose of this policy is to establish that certain requirements must be met In order for services to be covered, and are to be provided according to an individual written plan of service that has been developed by TBHS staff using a person-centered planning process.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Person-Centered Plan (PCP): Defined in the Michigan Mental Health Code to mean a process for planning and supporting the individual served that builds upon the individual's capacity to engage in activities that promote community life and honors the individual's preferences, choices and abilities. The process involves families, friends, and professionals as the individual served desires or requires.

PROCEDURES

According to Medicaid requirements, TBHS staff or its subcontractors, as applicable, are required to develop a preliminary written plan of service within 7 days of commencement of services (if person is hospitalized for less than 7 days, before discharge or release). The individual written plan of service shall:

- Include a treatment plan, a support plan, or both;
- The treatment portion of the plan should establish meaningful and measurable goals and objectives with the individual served;
- Address, as either desired or required by the individual served, the individual's need for food, shelter, clothing, health care, employment opportunities, legal services, transportation and recreation; and
- Be current and modified, when applicable.

TBHS and its subcontractors shall use reasonable good faith efforts to review at regular intervals the effectiveness of, and the provision of services under, an individual plan of service. Staff and

subcontractors are also responsible for fully reviewing and using good faith efforts to follow the Person-Centered Planning Best Practice Guideline (MDHHS Contract Attachment).

In each PCP written plan of service, any available natural support to assist the individual served to achieve his or her desired outcomes will be evaluated, identified and utilized. TBHS will make good faith efforts to allow each individual served to provide ongoing opportunities to express his or her dreams, desires and goals and to make choices regarding support and treatment options. TBHS will strive to inform individuals served of their rights to PCP and associated appeal options.

In some instances, an individual's dreams, desires, support or treatment choices pose issues of health or safety or exceed reasonable expectations of resource consumption or are not allowable costs. In those instances, TBHS will make good faith efforts to negotiate toward a mutually acceptable alternative that meets the outcomes intended. This information should be clearly reflected in the clinical record.

TBHS will also work in coordination with its subcontractors to effectuate this policy.

RELATED FORMS & MATERIALS

Person-Centered Planning Policy and Practice Guideline (MDHHS Contract Attachment)

REFERENCES/LEGAL AUTHORITY

Michigan Mental Health Code, MCLA 330.1700(g) and 330.1712
MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement, Attachment
MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement
Michigan Medicaid Provider Manual
Michigan Administrative Code, Section 330.7199
Michigan Administrative Code, Section 330.2814

Revision Dates:
10/06/2014
10/06/2015
11/30/2016
09/17/2018
09/20/2022

Policy Section	Education	Policy Number	X-002-003
Subject	Medical Necessity	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that its staff and subcontractors, as applicable, use good faith efforts to comply with all government and private payer requirements regarding medical necessity and that they fully document medical necessity in the clinical record of the individual served.

PURPOSE

The purpose of this policy is to establish criteria of payment for services provided; Medicaid, Medicare and other third party payers require that these services be medically necessary.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

TBHS staff and subcontractors, as applicable, are responsible for fully reviewing and using good faith efforts to comply with "Medical Necessity Criteria for Medicaid Mental Health and Substance Abuse Services".

For purposes of Medicaid, medical necessity with regard to mental health and/or substance abuse services has been defined to mean services that are:

- Necessary for screening and assessing the presence of a mental illness, developmental disability and/or substance use disorder; and/or
- Required to identify and evaluate a mental illness, developmental disability or substance use disorder; and/or
- Intended to treat, ameliorate, diminish or stabilize symptoms of mental illness, developmental disability or substance use disorder; and/or
- Expected to arrest or delay the progression of a mental illness, developmental disability or substance use disorder; and/or
- Designed to assist the beneficiary to attain or maintain a sufficient level of functioning in order to achieve goals of community inclusion and participation, independence, recovery, or productivity.

Moreover, medical necessity determinations are based upon a person-centered planning process. TBHS staff and subcontractors, as applicable, are responsible for using professional and well-informed efforts so that services provided are necessary to meet the individual's mental health needs and are consistent

with the diagnosis, symptoms, and functional impairments of the individual as well as consistent with clinical standards of care.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement, Attachments
MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement
Medicaid Provider Manual

Revision Dates:
10/06/2014
10/06/2015
09/17/2018
09/20/2022

Policy Section	Education	Policy Number	X-002-004
Subject	Range of Services	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Berls
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that per Medicaid requirements, TBHS offer directly or per contract, a comprehensive array of services as set forth in the Mental Health Code MCL Section 330.1206.

PURPOSE

The purpose of this policy is to identify the conditions under which the services are to be covered by Medicaid and what those services are.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Michigan Medicaid Provider Manual: contains coverage, billing, and reimbursement policies for Medicaid, Children's Special Health Care Services, Healthy Michigan Initiative, Maternity Outpatient Medical Services (MOMS), and other healthcare programs administered by the Michigan Department of Health and Human Services.

PROCEDURES

Service Conditions/Requirements:

Mental health and developmental disabilities services (state plan, HSW, and additional/B3) must be:

- Provided under the supervision of a physician, or other licensed health professional whose profession is relevant to the services being provided. This includes professionals who are licensed or certified in Michigan in a human services field typically associated with mental health or developmental disabilities services. (Refer to Staff Provider Qualifications in Medicaid Provider Manual)
- Provided to the beneficiary as part of a comprehensive array of specialized mental health or developmental disabilities services.
- Coordinated with other community agencies (including, but not limited to; Medicaid Health Plans [MHPs], family courts, local health departments [LHDs], MI Choice waiver providers, school-based services providers, and local MDHHS offices).
- Provided according to an individual written plan of service that has been developed using a person-centered planning process and that meets the requirements of Section 712 of the Michigan Mental Health Code. A preliminary plan must be developed within seven days of the commencement of services or, if a beneficiary is hospitalized, before discharge or release. Pursuant to state law and in conjunction with the Balanced Budget Act of 1997, Section 438.10

(f)(6)(v), each beneficiary must be made aware of the amount, duration, and scope of the services to which he is entitled. Therefore, each plan of service must contain the expected date any authorized service is to commence, and the specified amount, scope, and duration of each authorized service. The beneficiary must receive a copy of his plan of services within 15 business days of completion of the plan.

- The individual plan of service shall be kept current and modified when needed (reflecting changes in the intensity of the beneficiary's health and welfare needs or changes in the beneficiary's preferences for support). A beneficiary or his/her guardian or authorized representative may request and review the plan at any time. A formal review of the plan with the beneficiary and his/her guardian or authorized representative shall occur not less than annually to review progress toward goals and objectives and to assess beneficiary satisfaction. The review may occur during person-centered planning.
- Provided without the use of aversive, intrusive, or restrictive techniques unless identified in the individual plan of service and individually approved and monitored by a behavior treatment plan review committee.

Covered Services:

For purposes of Medicaid, covered mental health services include:

- Behavioral Health Treatment Services/Applied Behavior Analysis
- Assertive Community Treatment
- Assessments
- Behavioral Treatment Review
- Child Therapy
- Clubhouse Psychosocial Rehabilitation Programs
- Crisis Interventions
- Crisis Residential Services
- Family Therapy
- Health Services
- Home-Based Services
- Individual/Group Therapy
- Inpatient Psychiatric Hospital Admissions
- Intensive Crisis Stabilization Services
- Intermediate Care Facility for Individuals with Intellectual Disabilities (ICF/IID) Services
- Medication Administration
- Medication Review
- Nursing Facility Mental Health Monitoring
- Occupational Therapy
- Outpatient Partial Hospitalization Services
- Personal Care in Licensed Specialized Residential Settings
- Physical Therapy
- Speech, Hearing and Language
- Substance Abuse
- Targeted Case Management

- Telemedicine
- Transportation
- Treatment Planning
- Wraparound Services for Children and Adolescents

Additional information on the above services can be found in the Michigan Medicaid Provider Manual, Chapter III, Mental Health/Substance Abuse. TBHS may provide other alternative health services in lieu of the covered services listed above and may use Medicaid payments for same. These services include: Community Inclusion and Integration Services; Crisis Response; Family Support Services; Housing Assistance; Peer-Operated Support Services; Prevention and Counseling Services; Specialized Behavioral Health Services for Children/Adolescents; and Additional Community Mental Health Responsibilities.

TBHS staff and subcontractors, as applicable, are responsible for fully reviewing the services referenced above and using good faith efforts to comply with the requirements contained therein. Staff or subcontractors with issues or questions concerning their responsibilities in these areas should seek guidance from their direct supervisor or the Compliance Officer.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Michigan Mental Health Code MCL Section 330.1206
Michigan Administrative Code Section 330.2005, et. seq.
MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement Sections 2
Michigan Medicaid Provider Manual, Chapter III

Revision Dates:
10/06/2014
10/06/2015
11/30/2016
09/17/2018
10/08/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-005
Subject	Medicaid Eligibility	Issue Date	04/06/2010
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that its staff and subcontractors, as applicable, whose job duties include eligibility verification, use good faith efforts to verify each eligibility of each individual served, prior to services being rendered.

PURPOSE

As the majority of services provided by TBHS are rendered to the Medicaid population and paid by Federal and State funds, TBHS understands the importance of having an accurate and timely Medicaid eligibility verification process. Accordingly, TBHS staff and subcontractors (including BABH employees), as applicable, are responsible for using good faith efforts to follow this policy and to fully review the source documents referenced.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

According to Medicaid requirements, providers should verify an individual's Medicaid eligibility before rendering services by requesting the individual's current Medicaid ID Card and its effective date. TBHS Financial Administration Policy III-002-005; "Verification of Eligibility of Individuals Served" refers to verification of consumer eligibility which occurs automatically through the EMMIT system.

Third Party Liability/Dual Eligibility Issues:

Per Federal Regulations, a provider is responsible for billing all available financial resources for payment, including Medicare, prior to billing Medicaid/allocating Medicaid funds towards the service. It is a provider's responsibility for questioning the individual served to determine the availability of any third-party resources. To this end, it is the policy of TBHS that its staff and subcontractors, as applicable, whose job duties include eligibility and related billing functions, use good faith efforts to follow the eligibility and billing guidelines of the Medicaid program outlined in the most recent Medicaid Provider Manual.

TBHS understands that the government is concerned about dual eligibility issues and thus it is the policy of TBHS that good faith efforts are used to determine and verify dual eligibility status of individuals served and to follow the policy that Medicaid is the payer of last resort. Accordingly, when an individual is entitled to Medicare and eligible for Medicaid, Medicare like other third parties payers, is the primary payer.

Spend-Down Issues:

Some individuals served that have Medicaid are classified as Medicaid Deductible, or "spend down," meaning that they have met all Medicaid eligibility criteria except that they have an excess income. These individuals may become eligible for Medicaid if they incur medical expenses each month equal to, or greater than, an amount determined by the local Department of Health and Human Services ("DHHS") worker to qualify for Medicaid.

In order for such individuals to become eligible, they (or the provider) must present proof of any medical expenses incurred to the local DHHS worker. The local DHHS worker will then review the individual's bills which have been incurred and determine the amount of the liability for the individual served and the first date of Medicaid eligibility.

Importantly, a provider is not permitted to provide individuals served that have a spend-down with a notice of a bill incurred if no services have been rendered. Accordingly, TBHS staff and subcontractors, as applicable, are prohibited from providing individuals served that have a spend-down with bills or notices of bills incurred when no services have been rendered by TBHS.

TBHS staff and its subcontractors, as applicable, whose job duties include eligibility verification are responsible for fully reviewing relevant chapters of the Medicaid Provider Manual provisions and using good faith efforts to comply with the Medicaid program spend-down requirements.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Michigan Administrative Code Section 330.2810
Michigan Medicaid Provider Manual
OIG Work Plan 2017, page 40
42 USC Section 1396a note
TBHS Financial Administration Policy III-002-005
TBHS Financial Administration Policy III-002-006

Revision Dates:
10/06/2014
10/06/2015
09/17/2018
10/16/2019
10/08/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-006
Subject	Cost Reporting	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Beam Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to submit an accurate cost report to the State of Michigan. TBHS shall implement education and monitoring efforts to achieve this end.

PURPOSE

As a cost reporting entity, TBHS understands that inaccurate cost reporting can lead to, among other potential liability and exposure, false claims liability under the Federal False Claims Act. Thus, TBHS strives to accurately review and monitor and educate staff on cost reporting issues.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

TBHS instructs its finance department that the following are important areas for purposes of enhancing its compliance efforts:

- Accurate Reporting of Allowable Costs
- Full Documentation to Support Allocation of Costs and Allowable Costs
- Appropriate Internal Claims Tracking/Control Process to Support Allocation of Costs and Allowable Costs
- Full Documentation to Support Clinical and Administrative Costs
- Timely (59 days or less) report and return of any overpayments from the federal government.

TBHS also recognizes that appropriate eligibility and service event verification is important for purposes of enhancing compliance in the cost reporting area and thus the department responsible for verification will be educated on this issue. Although finance department employees are not responsible for this function, they should be aware of the importance of the process.

In furtherance of its compliance efforts, TBHS' Finance Department will undergo monitoring and educational activities in connection with the cost reporting issues noted above in accordance with the Compliance Department Monitoring and Education Plan.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

MDHHS/CMHSP Managed Mental Health Supports and Services Contract Agreement Part II 7.8
OMB Circular A-87
Federal False Claims Act

Revision Dates:
05/31/2012
10/06/2015
09/17/2018
10/08/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-007
Subject	Marketing & Public Relations	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that all marketing and informational materials used by TBHS to describe or advertise its community mental health services will be accurate, truthful and non-coercive.

PURPOSE

As part of its compliance efforts, TBHS will assure that all marketing materials will comply with HIPAA/HITECH Rules and the MDHHS/CMHSP Managed Mental Health Supports and Services Contract and be available to the MDHHS for review.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted, as appropriate.

DEFINITIONS

Not applicable.

PROCEDURES

1. TBHS will engage in marketing or public relations strategies that offer complete and adequate information. TBHS staff and subcontractors, as applicable, are responsible for engaging in accurate and truthful marketing or public relations strategies, including:

    - Represent the TBHS Mission accurately and ethically.
    - Promote the elimination of stigma.
    - Advocate for individuals served by exhibiting respect and understanding for behavioral health conditions.
    - Represent, as appropriate, the services TBHS provides, and to whom services are intended.
    - Provide literature to the public that is accurate and representative of the types of services provided by TBHS.
    - Advertise TBHS programs and services accurately and professionally.

2. TBHS shall obtain prior authorized approval from the individual served to send to them any written communication that is intended to promote, purchase, or use a third party's products or services if TBHS receives financial remuneration from or on behalf of the third party in exchange for sending the communication, with a few exceptions:

    - Face to face communications
    - Promotional gifts of "nominal" value

- Refill reminders, adherence reminders, or other communications about a drug for the individual served
- Communications about health in general (e.g. encouraging wellness, routine tests)
- Communications about government or government-sponsored programs that benefit the public (e.g. eligibility for Medicare or Medicaid).

Any communications not delivered in person may possibly be subject to this requirement:

- Phone calls, faxes, mail, e-mail and text messages
- Appointment reminders
- Treatment reminders
- Alternative treatments
- Health care products or services

a. TBHS shall maintain a log of marketing authorizations and identify those for which there is financial remuneration being provided by a third party.

b. The individual served shall also be advised of his or her right to opt out and revoke the authorization at any time.

3. If appropriate, TBHS may use, or disclose to a business associate, the following PHI for the purposes of its own fundraising without an authorization:

- Demographic information relating to an individual served(name, address, other contact information, age, gender, and date of birth).
- Dates of health care provided to an individual
- Department of service information
- Treating physician
- Outcome information
- Health insurance status

a. Each fundraising communication shall include information on how the individual served can opt-out of future fundraising communications, which shall not place an undue burden (e.g. too costly or complicated) on them.

b. TBHS shall not condition treatment on the individual's choice with fundraising communications.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

MDHHS/CMHSP Managed Mental Health Supports and Services Contract, Section 6.3.3
CARF Behavioral Health Standards Manual 2022
45 CFR Parts 160 and 164: HIPAA/HITECH

Revision Date:
08/05/2011
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/17/2018
10/16/2019
10/14/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-008
Subject	Collection of Co-Payments & Deductibles	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to use reasonably good faith efforts to collect all applicable co-payments and/or deductibles owed by its non-Medicaid individuals served.

PURPOSE

The purpose of this policy is to ensure the presence of a process that addresses service payment for individuals served not possessing Medicaid coverage.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs.

DEFINITIONS

Not applicable.

PROCEDURES

General Guidelines:

Refer to Financial Administration Policy III-002-001, "Ability to Pay" and III-002-002, "Accounts Receivable-Consumer" for full details on determining an individual's responsibility with respect to establishing an ability to pay for services rendered.

1) Financial liability for services is determined by either completion of the total financial situation of the individual served or with the application of the ability to pay (ATP) schedule referenced in Michigan Mental Health Code Chapter 8 section 330.1818 and section 330.1819.

2) The ATP determination is to be made in accordance with the policies referenced above.

3) The determination of ATP shall not impose any undue financial burden on the individual, spouse, or parent of a minor child.

4) TBHS shall make good faith effort to collect fees that are earned. TBHS, however, may forgive a co-payment or deductible in consideration of a particular individual's special financial hardship. TBHS recognizes that this forgiveness must be in good faith, be based on the special financial need of the individual served and must not be used routinely. TBHS also recognizes that such waivers of co-payments and deductibles will not be offered as part of an advertisement or solicitation. All write-offs require approval of the Chief Financial Officer.

5) TBHS shall use good faith efforts to document financial hardship for those cases in which it is granted.

6) For Medicaid eligible individuals served who have Medicare coverage, TBHS is responsible for any Medicare coinsurance and deductible payments for specialty services.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

42 USC Section 1320a-7b
31 USC Section 3729
59 FR 65372, Publication of OIG Special Fraud Alerts
MDHHS/CMHSP Managed Mental Health Supports and Services Contract, Section 6.6
TBHS Financial Policies III-002-001, III-002-002

Revision Dates:
10/06/2015
09/17/2018
10/16/2019
10/14/2020
09/20/2022

Policy Section	Education	Policy Number	X-002-009
Subject	Review Procedures For Contractual/Ownership Arrangements	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that all of its contracts and relationships are in compliance with the Federal Fraud and Abuse Laws: Federal False Claims Act, Deficit Reduction Act, Stark and HIPAA laws, as applicable.

PURPOSE

The purpose of this policy is the appropriate review of any subcontracts TBHS has with other providers.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

1. TBHS will consult legal counsel, when appropriate, to review its contracts and relationships in light of the Federal Fraud and Abuse Laws: Federal False Claims Act, Deficit Reduction Act, Stark and HIPAA laws.

2. TBHS shall execute all provisions of its contract with the Michigan Department of Health and Human Services, including subcontracted services. TBHS will consult legal counsel, when appropriate, to review its subcontracts in light of its direct contractual arrangements with the State and its compliance responsibilities.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
10/06/2015
09/20/2022

Policy Section	Education	Policy Number	X-002-010
Subject	Claim Preparation & Submission	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to use reasonable good faith efforts to ensure that its claims, as well as those of its subcontractors, are fully and accurately prepared and, when applicable, submitted in accordance with third party payer requirements.

PURPOSE

The purpose of this policy is guidance with respect to claims preparation and billing in accordance with the appropriate payer requirements.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

As a cost-reporting entity, TBHS prepares some claims that are not submitted to any third-party payer but are used for internal documentation purposes. These claims should include all necessary information for cost-reporting purposes, including the appropriate diagnostic code (from current diagnostic coding manuals, e.g. ICD-10, DSM-5), activity code, and, as applicable, service begin/end time, and be prepared with access to the medical record of individuals served and any authorization(s) for services.

TBHS also prepares some claims that are prepared and submitted directly to third-party payers, such as Medicare, Medicaid Children's Waiver, and private insurance companies. These claims shall be prepared and billed in accordance with the third party requirements. These claims should be prepared with access to the medical records of individual's served, any authorization(s) for services and appropriate third party payer manuals. Claims submitted to the Medicaid Children's Waiver shall be in accordance with Chapter III of the Michigan Medicaid Provider Manual.

TBHS will work in coordination with its subcontractors to effectuate their adherence to this policy. A subcontractor's submittal of claims to TBHS shall constitute the subcontractor's verification that the services have been completed in compliance with this policy and all reimbursement requirements of TBHS and Medicaid. If a subcontractor submits a claim for services rendered that is in the format specified by TBHS and can be processed without obtaining additional information from the subcontractor or a third party, TBHS shall make timely payments to said subcontractor in accordance with the MDHHS/CMHSP Managed Mental Health Supports and Services Contract.

It is the internal goal of TBHS that claim-preparing employees with questions seek assistance from his or her direct supervisor, the health care provider who provided the services and/or TBHS management. Claims should be held and, if applicable, not submitted until appropriate clarification is obtained.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Michigan Medicaid Provider Manual, Chapter III
MDHHS/CMHSP Managed Mental Health Supports and Services Contract, Section 6

Revision Date:
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-001
Subject	Complaints from Individuals Served	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to utilize a Privacy Officer that will be responsible for receiving all complaints from individuals served regarding TBHS' privacy policies or alleged breaches of the privacy policies.

PURPOSE

The purpose of this policy is to investigate all complaints from individuals served pertaining to alleged breaches of the individual's privacy and recommending whether disciplinary actions should be taken against employees as appropriate.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Receiving Complaints:

The Privacy Officer shall be identified/assigned by the TBHS CEO. It is the responsibility of the Compliance Department to implement the responsibilities of this function. The Privacy Officer will be responsible for receiving all complaints from individuals served regarding TBHS' privacy policies or alleged breaches of the privacy policies. The Privacy Officer will also be responsible for investigating all complaints and recommending whether disciplinary actions should be taken against employees as appropriate.

This action will be coordinated with TBHS' already existing Recipient Rights System.

No Intimidation, Retaliation, or Request to Waive Rights:

Individuals served have a right to file complaints with the Privacy Officer and with the government. TBHS employees must act cooperatively with individuals served who wish to file a complaint. TBHS will not intimidate, threaten, coerce, or take any retaliatory acts against the individual for filing a complaint with the Agency or with the government. For example, employees cannot try to persuade an individual not to file a complaint. TBHS will not treat individuals who file complaints differently than other individuals served.

TBHS will not ask individuals served to waive their right to complain to the government or to the Agency.

TBHS will not retaliate against any individual(s) (including employees) for participating in the complaint (for example, TBHS will not discipline or terminate an employee for cooperating or testifying in a government investigation).

Duty to Mitigate:

If TBHS learns that there has been a breach of its privacy policies or that any HIPAA requirement has not been met, it will try to reduce the harmful effects caused by the breach (for example, if an employee wrongfully discloses information of an individual served to a third party, the third party will be notified and asked to stop using or disclosing the information).

Complaints Against a Business Associate:

TBHS will also take complaints from individuals served regarding alleged violations by TBHS' business associates. The Privacy Officer will investigate all such complaints. If, upon investigation of a complaint, the Privacy Officer identifies that the business associate has materially violated a term of its agreement with TBHS with respect to protection of privacy of the individual served, the business associate will be contacted and asked to stop or correct the activity involved. If the business associate does not respond to these requests, TBHS will take steps to terminate the contract. If termination is not feasible, TBHS shall report the problem to the Department of Health and Human Services Office for Civil Rights.

Documentation of Complaints:

The Privacy Officer will be responsible for documenting all complaints from individuals served and the disposition of the complaints. This documentation must be kept for a period of at least six years.

1. If an individual served approaches an employee about filing a complaint regarding a privacy issue, the individual should be referred to the Privacy Officer.
2. The Privacy Officer is responsible for documenting the individual's complaint. The disposition of the complaint should also be noted, and the complaint/disposition kept for a period of at least six (6) years.
3. The Privacy Officer is responsible for investigating the individual's complaint and for educating and recommending discipline of workforce members as necessary and in keeping with TBHS' established Personnel Policies related to the discipline process. The Privacy Officer is also responsible for determining what steps need to be taken to mitigate harmful effects to the individual served and for taking these steps in a timely fashion.
4. If the complaint involves a business associate, the Privacy Officer is responsible for addressing the issue with the business associate, along with the TBHS Contract Manager.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-013
Mental Health Code, Section 776
45 CFR §164.504 (e)(1)
45 CFR §164.530

Revision Dates:
10/06/2014
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-002
Subject	Safeguarding Faxes	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to safeguard protected health information (PHI) that is sent and received by use of a fax machine.

PURPOSE

The purpose of this policy is to ensure that no PHI is left unattended at a fax machine by an employee responsible for acceptance or transmission of the PHI.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

1. TBHS will take reasonable safeguards to protect fax communications including:

   - To the extent that it is reasonable, locating fax machines in areas that are not a high traffic area and not viewable or accessible by visitors.
   - To the extent that it is reasonable, limiting access to the fax machines to certain employees.

2. Employees will take reasonable steps to ensure that fax transmissions are sent to their intended destinations, including:

   - Double checking fax numbers before dialing.
   - If an employee becomes aware that a fax has been misdirected, contacting the recipient and asking them to discard the misdirected fax.
   - Making sure that all faxes are accompanied by a fax cover sheet that contains a confidentiality statement.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-003
Subject	Minimum Necessary/Need to Know Protocols for Routine Disclosures to Medicaid & Other Health Plans	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to determine what information should be submitted to support a claim. TBHS will determine what information is minimally necessary to achieve the results for which the information is being requested.

PURPOSE

The purpose of this policy is to ensure there is an appropriately established process to provide information to third party payers (e.g., Medicaid, Medicare, Blue Cross, etc.) as required by contracts and/or subscriber agreements with the payer.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted (if applicable).

DEFINITIONS

Not applicable.

PROCEDURES

Disclosures Specifically Required by Health Plans:

TBHS will rely upon a health plan's representations regarding the information that is needed for a claim, including representations that are contained in a policy, a provider agreement, or in a health plan newsletter or bulletin. For example, to the extent that the health plan makes representations that the information is necessary, the following information may be provided as part of a claim to a health plan:

- Date(s) of service
- Demographic information of the individual served
- Information regarding the insurance contract number, plan number, group number, etc.
- Diagnosis and/or procedure codes
- Information regarding medical history
- Referral or pre-certification information
- Other information requested by the health plan such as portions of the medical record related to the dates of service at issue

Unspecific Requests by Health Plan:

There may be situations where TBHS must make a disclosure of protected health information that has not been specifically requested by the third party payer. For example, TBHS may need to determine what information should be submitted to support a claim or defend an audit. In these situations, TBHS will determine what information is minimally necessary to achieve the results for which the information is being requested. Information beyond that which is minimally necessary will not be disclosed. For example, if a particular date of service is being questioned, it may be necessary to submit excerpts from the date of service in question, as well as information from previous or subsequent visits that support medical necessity, plan of care, etc. Although the entire medical record should not be routinely submitted, it may be where necessary.

1. For the purposes of claims submission, information required or requested by the health plan should be submitted.
2. Employees can rely upon representations from health plans regarding the information that is required.
3. If TBHS needs to submit additional information, employees determine what information is necessary to support the service in question.
4. If an employee has a question as to the amount of information that should be provided for a certain disclosure, he or she should consult with the Privacy Officer.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Mental Health Code, Section 748

Revision Dates:
10/06/2014
10/08/2020
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-004
Subject	Uses & Disclosures Restricted to-Minimum Necessary Information	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Betts
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) in accordance with the Pre-Paid Inpatient Health Plan (PIHP) Privacy Policy and in support of the Organized Health Care Agreement (OHCA), when using and disclosing Protected Health Information (PHI) for payment and health care operational purposes, to make reasonable efforts to limit the amount of PHI of individuals served used and disclosed to that which is minimally necessary to accomplish the intended purpose of the use.

PURPOSE

The purpose of this policy is to ensure that TBHS is in compliance with minimum necessary information requirements relative to employee access to PHI and EPHI (electronic protected health information).

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Internal Access of PHI:

For uses of information within TBHS, TBHS has determined that employees need access to information as follows (including access to EPHI):

Physicians: Full access to protected health information of individuals served.

TBHS Social Workers or Other Treating Professionals: Full access to medical records and other PHI of individuals served who they treat with the condition that medical records and information must only be accessed for appropriate purposes (e.g., in furtherance of treatment of the individual served or communicating with the individual served, to facilitate information necessary for billing purposes).

Front Office Staff: Access to all scheduling information of individuals served and sign in logs and sheets. Front office staff shall be granted access to medical records as required by specific job functions. The supervisor can grant additional levels of access as necessary.

Medical Records Staff: Medical records staff shall be granted access to medical records and other PHI of individuals served only as required by specific job functions. The supervisor can grant additional levels of access as necessary.

Billing Office Staff/Finance Staff: Access to charge slips, activity logs, and scheduling information of individuals served. Coding and billing personnel shall not have free access to all medical records of individuals served. Coding/billing personnel are permitted to access medical records of individuals served when necessary to obtain pertinent components of the record required to be submitted for payment. The supervisor can grant additional levels of access as necessary.

Disclosures to Third Parties:

Disclosures of PHI that do not occur on a routine basis must be reviewed individually to determine the minimum amount of information that must be disclosed to achieve the stated purpose of the disclosure, based upon the following criteria:

- Determine whether the requestor was specific about the type of information that is needed (e.g., demographics, financial/billing, portions of the medical record).
- If the requestor was not specific, ask the requestor specifically what information is needed and why.
- If the requestor requests the entire medical record, ask the requestor to justify why the entire medical record is needed. Employees should not disclose an entire medical record until satisfactory justification is provided by the requestor. Employees should seek approval from their supervisor, as applicable, before disclosing an entire medical record.
- Determine whether the requestor is a person who can be relied upon:
  - When making a permissible disclosure to a public official TBHS may rely on the public official's representations regarding the amount of information needed.
  - When making a disclosure to another covered entity (e.g. a provider, health plan or clearinghouse) TBHS may rely on the requestor's representations regarding the amount of information needed.
  - TBHS may rely upon the professional judgment of a business associate to determine what information is needed for the performance of professional services (e.g., an accountant or attorney).
- If the requestor is a person whose representations can be relied upon, then the employee may disclose the requested information.
- If the requestor is not a person whose representations can be relied upon, and the employee has any question regarding the appropriateness of the scope of the request, the employee should ask the supervisor for approval to disclose the information.
- Employees are responsible for verifying the identity of a requestor if the employee does not know the requestor.

Application of the Minimum Necessary Rule Where TBHS is the Requestor:

HIPAA requires TBHS to restrict requests for information to the minimum necessary to achieve the intended purpose of the requested disclosure. Requests for protected health information should be made subject to the following criteria:

- Requests should be as specific as possible with respect to the amount of information needed.
- Requests should not be for entire medical records unless absolutely necessary.
- If the information is being requested for treatment purposes, the entire medical record may be requested.
- Employees should be prepared to provide justification for the scope of the request.

- All employees are responsible for reviewing the policy (see above) on what information they are permitted access to. If employees believe that they have a need to access additional information, they should contact their supervisor. The supervisor may contact the Privacy Officer for consultation, as appropriate.
- If an employee makes a request for information from another covered entity, the request should be specific and limited in scope consistent with the criteria set forth in this policy.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
Mental Health Code, Section 748,946
45 CFR §164.502(b)
45 CFR §164.514(d)
45 CFR §164.514(h)

Revision Dates:
10/06/2014
11/30/2016
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-005
Subject	Notice of Privacy Practices	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Banks
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that all individuals served (or their personal representative) will be given TBHS' Notice of Privacy Practices (the "Notice").

PURPOSE

The purpose of this policy is to ensure that TBHS provides notice to each individual served of the ways in which TBHS may use and disclose the individual's personal health information, the individual's rights under HIPAA and that TBHS' duties under HIPAA are in compliance with minimum necessary information requirements.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

The Notice must be provided on or before the first encounter with the individual served (e.g., the first service delivery date). The Notice does not have to be provided on subsequent visits or service dates, but copies must be available at physical service site locations and provided to any individual served upon request.

The Notice must be posted in a clear and prominent location at service delivery sites (in such a place where the individual served would reasonably be expected to look- e.g., reception or waiting areas).

At the time the individual served is provided with the Notice, TBHS will make a good faith effort to obtain a signed or initialed Acknowledgement from the individual or his or her personal representative. The Acknowledgement is a statement that the individual served has received the Notice. If a signed or initialed Acknowledgement cannot be obtained, TBHS will document the good faith efforts that were made to obtain the Acknowledgement and the reason why the Acknowledgement could not be obtained. If the Acknowledgement cannot be obtained because of an emergency, TBHS will make good faith efforts to obtain the signed or initialed Acknowledgement as soon as practicable after the emergency situation has ended.

In the event that TBHS' Privacy Notice is revised, TBHS will provide a copy of the revised notice to all active individuals served and obtain a signed Acknowledgement from the individual served or his/her personal representative. TBHS will maintain a copy of the HIPAA Privacy Notice, any revisions to the notice and all acknowledgements by individuals served for a minimum of six years.

The Privacy Officer is responsible for maintaining a file with the version of the HIPAA notice and all other HIPAA materials.

TBHS will have copies of the HIPAA Privacy Notice and HIPAA Privacy Notice Summary Sheet available at all Agency buildings. All front desk or reception staff personnel will be responsible for distribution of notices and procuring each individual's or their personal representatives' signature on the acknowledgement sheet. A log will be kept at each site of those individuals who have completed this requirement. It is the responsibility of the TBHS Privacy Officer to ensure that the Notice is properly posted at service locations.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

45 CFR §164.520 (Notice)
45 CFR §164.530 (j)(1)(2)(Documentation and retention)

Revision Dates:
11/30/2016
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-006
Subject	Personal Representatives	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that under HIPAA, if an individual has the authority to act on behalf of the individual served under Michigan law, that person is considered a personal representative.

PURPOSE

The purpose of the policy is to ensure a process is in place for TBHS employees to utilize the personal representative as the individual served for purposes of signing HIPAA forms and exercising HIPAA rights.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Employees who have responsibilities for getting forms signed or with regard to individuals served exercising their rights under HIPAA are responsible for reviewing and following this policy. Employees with questions as to whether or not an individual is a personal representative of an individual served should contact the Privacy Officer.

MINORS

Determination of Personal Representative Status for Unemancipated Minors:

For unemancipated minors, the following are personal representatives under Michigan Law:

- The child's custodial parent.
- The child's non-custodial parent unless there is a court order limiting the non-custodial parents' access to medical records. (Note: the custodial parent may object to the release of mental health records to the non-custodial parent).
- The child's legal guardian.
- A person with whom the care of the child has been entrusted by the child's parents and whom the parents have authorized in writing to consent to medical treatment on the child's behalf.
- Person standing "in loco parentis" (a person who has legal or physical custody of the minor and is providing support and care for the minor).
- A child care institution, or child care organization with written authority to consent to routine, non-surgical medical care of the child.

- For children whose parents' parental rights have been terminated, the probate court or agency having jurisdiction over the child.

Determination of Emancipation

If a minor is emancipated, he or she is treated like an adult. Under Michigan law, a minor is emancipated if:

- He or she is validly married.
- He or she is 18 years of age.
- He or she is on active duty with the armed forces of the United States.
- There is a court order for emancipation.
- The minor is in police custody and the minor's parent or guardian cannot be located (please note that emancipation in this context is limited to consent for routine, non-surgical medical care or emergency medical treatment).
- The minor is incarcerated, and the minor's parent or guardian cannot be located (please note that emancipation in this context allows consent for all medical care with the exception of vasectomies or other procedures related to reproduction).

Control of Medical Information by an Unemancipated Minor:

In most situations, the parent or legal guardian of an unemancipated minor will control the flow of the minor's health information (e.g., request access, request restrictions, request amendment, sign authorizations, etc.).

An unemancipated minor can control his or her own health information (including a request that information not be provided to parents) in the following limited situations:

- The minor and the parent, guardian, or person acting in loco parentis entered into an agreement for confidentiality with respect to such treatment.
- Mental health services provided to a minor patient age 14 or older may not be disclosed to the parent, guardian, or person acting in loco parentis unless the mental health professional treating the minor determines that there is a compelling need for disclosure and the minor is first informed.

There are other situations where the minor can sign his or her own informed consent for treatment and exercise all rights under HIPAA, but for medical reasons cannot preclude TBHS from informing the parents or guardian regarding the treatment. Specifically, based upon Michigan law, the minor can consent to treatment and can exercise rights under HIPAA with regard to substance abuse treatment. However, for medical reasons, the treating physician or member of the medical staff of a clinic or other health professional, and on the advice and direction of the treating physician, may, but is not obligated to, inform the parent, guardian or person in loco parentis as to the substance abuse treatment given to or needed by a minor. The information can be provided even if the minor expressly refuses.

Incapacitated Adults

For adults, the following are personal representatives:

- A court appointed guardian.

- Where there is no court appointed guardian and the individual served cannot make his or her own decisions: a patient advocate (designated in writing by the patient in a durable power of attorney document) or a surrogate decision maker (such as a family member).

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-014
Mental Health Code, Section 702
45 CFR §164.502(g) (personal representatives)
MCL 330.1707 (parent or guardian not to be notified of mental health services provided to minor)
MCL 333.5653 (definition of patient surrogate)
MCL 333.6121 (minor can consent to substance abuse treatment)
MCL 333.9132 (minor can consent for prenatal and pregnancy related care)
MCL 600.2157 (deceased's heirs at law are personal representatives)
MCL 700.5215 (minor's legal guardian)
MCL 700.5313 (appointment of guardian of legally incapacitated individual)
MCL 700.5511 (patient advocate)
MCL 722.124a (child care organizations and institutions)
MCL 722.30 (non-custodial parents' right to access records)
MCL 722.904 (judicial waiver of consent for abortion)
Attorney General Opinion No. 7092 (October 16, 2001) (custodial parent may object to release of mental health records to non-custodial parent).
Ingham County Dept. of Social Services v. Curry, 113 Mich. App. 821 (1982) (parents may execute and sign authorization allowing relative in whose care child has been entrusted to consent to any medical treatment child may require).
Devilbiss Company v. Hush, 77 Mich. App. 639 (1977) (common law definition of "in loco parentis").
Young v. Oakland Gen. Hosp., 175 Mich. App. 132 (1989) (patient surrogate)

Revision Date:
10/08/2020
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-007
Subject	Reasonable Safeguards	Issue Date	04/06/2010
		Revision Date	09/20/2022
		Approved By	[signature]
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that TBHS will make reasonable efforts to prevent uses and disclosures that are not permitted in the Privacy Rule.

PURPOSE

Reasonable safeguards must be taken to prevent disclosure of information beyond that which is minimally necessary and to prevent disclosure of information to persons who do not need the information to perform their job function. TBHS also has addressed reasonable safeguards in the TBHS Recipient Rights and Information Systems & Technology Use Policies (see authorities at the end of the policy). This includes having reasonable administrative, technical and physical safeguards in place to prevent such impermissible uses and disclosures. In determining what safeguards are "reasonable", TBHS will use the viewpoint of a prudent health care professional.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Electronic Media: Storage media including memory devices in computers and any removable medium. Transmission media includes internet, extranet and networks.

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and maintained in electronic media.

Protected Health Information (PHI): Individually identifiable health information.

PROCEDURES

Safeguarding Oral & Written Communications & Computer Records

TBHS recognizes that there are uses and disclosures that could occur that do not require a signed HIPAA authorization from the individual served or the personal representative of the individual served, as applicable. TBHS shall continue to obtain written consent from the individual served under state law for disclosures of personal health information made outside the agency.

Some of the reasonable safeguards TBHS will take include:

- Employees are responsible for taking reasonable precautions to keep medical records of individuals served out of view of other individuals served and those who do not need access to perform their jobs.

- Employees are responsible for making reasonable attempts to keep conversations quiet when personal health information is being discussed among employees in a common area.
- Employees are responsible for taking individuals served to a private area or speaking quietly when discussing protected health information (for example, extensive discussions regarding treatment, medical history, and current problems should not be conducted in common areas).
- Employees are to avoid talking about individuals served outside of the Agency or service sites (for example, in elevators, hallways, or at restaurants during lunch hour).
- Employees are responsible to log out of the electronic health record (EMMIT) when it is not in use and at the end of the work day. Employees are responsible for putting charts away at the end of the day.
- If PHI is to be transported, it must be prepped to ensure no identifying information is visible. Locked cases are provided for transporting PHI externally between locations. The cases are not to be unlocked or the PHI removed until staff is in a secure area.
- Employees are responsible for taking precautions and using judgment when leaving messages on answering machines.
- TBHS will only send correspondence such as appointment reminders in envelopes and not on exposed postcards. The envelope used will be of a secure type and only the TBHS return address will be on it, with no agency name.
- Employees are responsible for preventing the use of protected health information when communicating via e-mail or when posting information on the Internet (e.g., discussion groups, list serves).
- Employees are not permitted to discuss personal health information of individuals served for inappropriate purposes such as gossiping.
- Employees are responsible for properly safeguarding PHI and EPHI that is contained in files and computers when traveling and when the information is at home.

Safeguarding Computers:

In addition to the HIPAA security regulations, the HIPAA privacy regulations require that technical safeguards be put in place to safeguard protected health information (PHI). If a computer contains electronic protected health information (EPHI), access to the computer should be protected by the use of passwords. Each employee is responsible for keeping his or her password confidential. Employees should not use their name as a password or any other word that could be easily guessed by others. Employees should not share computer passwords. Employees should logout of the computer if the computer will be left unattended. Employees agree that they will only access the computer for information that they need to know and will not attempt to access the computer if they are not authorized to do so.

- Employees should take reasonable precautions to safeguard information from unintended disclosure.
- Employees should take reasonable precautions to safeguard information so that only the minimal amount of information necessary to serve the stated purpose is either used or disclosed.
- Employees should take reasonable precautions to safeguard information so that information is not disclosed to people who do not have a need to know the information.
- If employees do not have a need to access a computer, they should not have a password and should not try to gain access to the computer system.
- If an employee has a computer password, he or she should not share the password with anyone else, including other employees and should not post the password on or near the computer.

- Employees who have the opportunity to choose their own computer password should take precautions so that the password is not something that could be easily guessed.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
TBHS Management of Information Systems Policy XI-001-003
45 CFR §164.530
45 CFR §164.514

Revision Dates:
08/05/2012
06/01/2012
10/06/2014
11/30/2016
10/08/2020
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-008
Subject	Individuals Served Right to Request Access or Amendment to Records	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 5

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to allow an individual served to inspect and/or be provided a copy his or her own medical records, billing records, or other records used by TBHS.

PURPOSE

The purpose of this policy is to establish a process for TBHS to act on all requests from individuals served/legal guardians for access or inspection of the medical record of the individual served.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Right to Request Access to Records:

If TBHS does not maintain the requested information, but knows where the requested information is kept, TBHS must inform the individual where to direct the request for access.

The individual served may request that the information be provided in a particular format of his or her choosing (e.g. electronic or paper), TBHS will comply if the information can be readily made available. If TBHS cannot readily provide the requested format, TBHS will work with the individual to reach agreement on an alternate format in which to provide the copy of the PHI.

TBHS may provide the individual served with a summary of the requested information instead of the actual information if the individual agrees to accept a summary and agrees to accept any charges imposed by TBHS for preparation of the summary.

TBHS may charge reasonable fees for copying, postage, and preparation of a summary (if the individual has agreed to a summary). If the individual served wishes to inspect the information instead of receiving a copy, TBHS will arrange for a convenient time and place for the inspection. It is the policy of TBHS to have the program supervisor, the Health Information Specialist or another Medical Records staff remain with the individual as he or she reviews the record.

TBHS must act on all requests for access or inspection within thirty (30) days by either sending a denial letter or providing the requested access. If the request is from the Michigan Department of Health and Human Services (MDHHS) or Child Protective Services (CPS), response is required within fourteen (14) days, according to TBHS Recipient Rights Policy, VII-001-019. If the requested information is stored

off-site, TBHS may have up to sixty (60) days to provide access. If TBHS cannot meet these time frames, TBHS can receive one thirty (30) day extension by sending the individual served a letter including the reason for the delay and the date by which TBHS will comply with the request.

If the request has been for electronic PHI (EPHI), TBHS may email (unencrypted) the requesting individual their EPHI provided this method is specifically requested by the individual, on the condition they have been advised of the risks involved and still prefer to receive the message by unencrypted email. TBHS shall ensure that the individual has signed a Request for Information form which provides a warning of using this method of delivery of sensitive electronic information. TBHS is not responsible for safeguarding information once delivered to the individual served.

Denial of Consumer Request for Access:

TBHS can deny access for any of the reasons set forth below. If the reason for the denial applies to only a portion of the requested information, then the request should be granted to the extent possible. If a request is denied, TBHS must provide a letter.

Non-Reviewable Grounds for Denial:

In the following circumstances, TBHS is not required to provide access to the individual served and the individual served does not have the right to request a review of the denial:

- The request is for psychotherapy notes. For the purposes of HIPAA, psychotherapy notes include only those notes that are separated from the rest of the medical record of the individual served and document or analyze conversations during a counseling session. Please note that the rest of the medical record, even though it may include mental health diagnoses, etc. is not considered to be "psychotherapy notes" and, therefore, must be disclosed to the individual served (unless another ground for denial exists);
- The request is for information compiled in anticipation of a civil, criminal or administrative proceeding;
- The information requested was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information;
- TBHS is providing health care services on behalf of a correctional institution and the individual served is an inmate (if providing the records would jeopardize the health, safety, security, custody, or rehabilitation of the individual, other inmates or the safety of any employee or agent of the correctional institution).
- The request is for information collected and maintained in the course of research that includes treatment and the individual served agreed to the denial of access when consenting for the research study. Please note that denial under these circumstances can only be temporary and the individual served must be afforded access once the research study has been completed.

Reviewable Grounds for Denial:

In the following circumstances TBHS may refuse to grant access to the individual served, but must give the individual served the right to have the denial reviewed by another licensed health care professional who did not participate in the original denial:

- A health care professional determines that allowing access to the information would be reasonably likely to endanger the life or safety of the individual served or another person;
- The requested information refers to another person (other than a health care provider) and a licensed health care professional determines that the access requested is reasonably likely to cause substantial harm to this other person;
- The request is made by a personal representative and a licensed professional has determined that the requested access is reasonably likely to cause substantial harm to the individual served or another person.

Right to Request Amendment to Information for individual served:

An individual served has the right to request that his or her information be amended. TBHS requires that the individual served submit the request in writing and that the individual provide a reason to support the requested amendment. TBHS must either accept or deny a request from an individual served within sixty (60) days of the request. TBHS can obtain one thirty (30) day extension if it provides the individual served with written notice of the reason for the delay and the date upon which the information will be provided. If the request is denied, TBHS will provide the individual served with a written letter explaining the basis for the denial, the right of the individual to submit a written statement disagreeing with TBHS, the right of the individual to ask that his/her statement be included with any future disclosures of the record at issue, the process for the individual to request the Agency to review the denial and the process for the individual to file a complaint with Health Information Specialist, if the consumer chooses.

Accepting a Request for Amendment:

If TBHS agrees to the requested amendment, TBHS must do the following within the 60-day time frame (or 90-days if the extension is requested):

- Make the requested amendment.
- Inform the individual served that the amendment has been accepted.
- Obtain from the individual served the names of all individuals who received the protected health information, obtain the agreement of the individual served to notify these individuals of the amendments, and inform the individuals of the amendments.
- Identify and inform all persons or entities who have the information that is the subject of the request who have relied upon this information, or can be expected to rely upon this information in the future to the detriment of the individual served.

Denying a Request for Amendment:

The following are grounds for denial:

- TBHS believes that the record is accurate and complete.
- Access to the medical record has been denied for one of the reasons set forth above in the access section of the policy
- The information is not part of a designated record set (i.e., not part of the medical records, billing records, or other records used to make decisions about the individual served).
- The information was not created by TBHS (e.g., medical records from another provider).

If the request is denied, TBHS must provide the individual served with a written denial letter. The individual served has the right to submit a statement of disagreement and TBHS has the option of responding with a written rebuttal. The Health Information Specialist or designee shall prepare a written rebuttal in response to all statements of disagreement.

Inclusion of Amendment Information in Future Disclosures:

If the individual submits a statement of disagreement, the above information (request for amendment, denial, statement of disagreement, and rebuttal) or a summary of this information must be included with any subsequent disclosure of the information that is the subject of the amendment request. If the individual served does not submit a statement of disagreement, he or she may request that the amendment request and denial be submitted with any future disclosures of the information that is the subject of the amendment request.

If a future disclosure must be made in standard format, the additional information described above may be submitted separately.

Documentation Requirements:

- The request for amendment
- The denial (if applicable)
- The individual's served statement of disagreement (if applicable)
- The TBHS' rebuttal to the statement of disagreement (if applicable)

Process for Requesting Access or Amendment to Record:

1. Employees should inform individuals served that all requests for access or amendment should be in writing and either mailed or hand-delivered to the attention of the Health Information Specialist or designee. The request should be signed and dated by the individual served, or the legal representative of the individual served. If requests are hand-delivered to the office, all employees are responsible for making sure that the request is signed, dated and given to the Health Information Specialist or designee.
2. The Health Information Specialist, either personally or by delegation, will be responsible for keeping a log of all requests and the deadline for the requested information and/or amendment.
3. If TBHS does not maintain the requested information, but knows where the requested information can be found, the Health Information Specialist is responsible for contacting the individual served to inform him or her of the location of the requested information.
4. If a request for inspection, copies, or amendment is denied, the Health Information Specialist must send the individual served a denial letter before the relevant deadline (thirty (30) days for inspection/copies on-site, sixty (60) days for inspection/copies offsite, and sixty (60) days for amendment).
5. If a request for inspection, copies, or amendment is accepted, the Health Information Specialist will be responsible for fulfilling all of the duties set forth in the policy within the applicable time frames.
6. If a thirty (30) day extension of the relevant time frame is necessary, the Health Information Specialist must send the individual served a letter explaining the reason for the delay and identifying the expected date by which TBHS will respond to the individual served.

7. If a request for inspection and/or copies is denied for grounds that are reviewable and the individual served seeks a review of the denial, the Health Information Specialist will arrange for an independent review by a licensed health care provider who was not involved in the denial.
8. If the individual served responds to a denial of a request for amendment with a written statement of disagreement, the Health Information Specialist will be responsible for preparing a written rebuttal and providing a copy of the rebuttal to the individual served.
9. The Health Information Specialist will be responsible for making sure that the following are included in the record of the individual served that was the subject of any request for amendment: the request, the denial, statement of disagreement and rebuttal. This information must always be included with subsequent disclosures of the information if the individual served submitted a statement of disagreement or asked that the request for amendment be included with future disclosures.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
Mental Health Code, Section 748
45 CFR §164.524 (inspection/copy)
45 CFR §164.526 (amendment)
MCL 330.1748

Revision Date:
08/05/2011
11/19/2013
10/06/2015
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-009
Subject	Rights of Individuals Served - Restrictions on Use of Protected Health Information	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that the individual served has the right to request that restrictions be placed on the use and/or disclosure of his or her protected health information (PHI).

PURPOSE

The purpose of this policy is to address a request for restrictions of their (PHI) by an individual served. If TBHS agrees to a request, the requested restriction must be honored unless there is an emergency situation.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

OCHA Statement

In support of the Organized Health Care Arrangement (OHCA), it is the policy of TBHS, as related to the Health Insurance Portability and Accountability Act (HIPAA) of 1996:

- that there are uses and disclosures of information of individuals served that could routinely occur at TBHS that do not require a signed HIPAA authorization from the individual served or the legal representative of the individual served, as applicable. TBHS personnel, however, shall continue to obtain the written consent of the individual served under State law for disclosures of information of the individual served made outside the agency.
- that when using and disclosing Protected Health Information (PHI) or for treatment, payment, and coordination of care, TBHS must make reasonable efforts to limit the amount of PHI of individuals served and Electronic Protected Health Information (EPHI) used and disclosed to that which is minimally necessary to accomplish the intended purpose of the use.

Right of Individuals Served to Request Restrict ions on Use of Protected Health Information :

The individual served has the right to request that restrictions be placed on the use and/or disclosure of his or her protected health information in connection with uses and disclosures for treatment, payment and coordination of care and when disclosing to family members. If the individual served requests, TBHS shall restrict disclosure of PHI if the PHI pertains solely to a health care item or service for which the individual served, or a party other than the health plan, has paid the provider in full. See also TBHS Recipient Rights Policy VII-001-019.

Exception: The individual served cannot request restrictions on uses or disclosures to the government for investigation of HIPAA compliance, information provided to law enforcement, pursuant to a court order, or for any of the special circumstances set forth in the Uses and Disclosures HIPAA policy.

TBHS has the right to refuse a s request by an individual served for restrictions. If TBHS agrees to a request, the requested restriction must be honored unless there is an emergency situation.

If a request for a restriction is denied, the individual served may then choose to continue treating with TBHS, discontinue treatment, or modify his or her request to the extent that it is acceptable to TBHS.

Termination of Restriction Agreement:

Once TBHS has agreed to a restriction, it may terminate the restriction as follows:

- For information that has already been created or received (e.g., existing medical records): TBHS can terminate its agreement to a restriction only if the individual served agrees to the termination. The individual's agreement must be documented in writing by the individual served or by an employee who received oral authorization from the individual served.

- For future information (that has not yet been created or received): TBHS can terminate its agreement by notifying the individual served that it will not continue with the agreed upon restriction for future uses and disclosures.

Right to Request Alternative Means of Communications:

The individual served may request that protected health information be communicated in a certain way (for example, he/she may request that communications not be made at his/her place of work, or that all bills be sent to a certain address).

TBHS must comply with all reasonable requests for alternative means of communications. Reasonableness must be determined by administrative considerations only. Employees are not permitted to ask individuals served the reason for the request.

It is the policy of TBHS that employees consult with the Health Information Specialist, or designee prior to making a determination that a request is unreasonable.

If a request is determined to be unreasonable, this information will be communicated to the individual served. The individual served will then be notified that they can either (1) modify their request for alternative communications to make it reasonable, (2) continue treating with TBHS with the understanding that the requested communications will not be honored, or (3) make the decision to treat elsewhere.

All requests for restrictions or alternative methods of communications (along with decisions to deny or accept) must be kept for a period of at least six (6) years.

Procedure for Request for Restrictions:

1. An employee receiving a request for a restriction on uses and disclosures or a request for an alternative method of communication of protected health information is responsible for communicating the request to the Health Information Specialist, or designee.

2. Employees are not permitted to ask an individual for an explanation as to why an alternative method of communication is being requested.
3. Employees should ask the individual served to put requests for alternative methods of communication in writing (employees may not require requests for restrictions be placed in writing). If the Individual served objects to the written request requirement, he or she should be referred to the Health Information Specialist. The Health Information Specialist, or designee may enforce the requirement that the request be placed in writing or can agree to document the request on behalf of the individual served.
4. The Health Information Specialist, or an employee designated by the Health Information Specialist, will be responsible for determining whether a request can be granted. The Health Information Specialist, or designee cannot refuse a request for alternative method of communications if the request is reasonable.
5. If a request by an individual served for either a restriction or alternative method of communication is refused,
the individual served must be informed of the refusal.
6. If a request is granted, the Health Information Specialist, or an employee designated by the Health Information Specialist, will be responsible for notifying staff of the restriction as necessary to comply with the restriction.
7. If a request is terminated, the Health Information Specialist, or designee will be responsible for notifying staff that the restriction has been removed.
8. The Health Information Specialist, or designee will be responsible for keeping copies of written consumer requests for a period of six (6) years.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
45 CFR §164.502(c)
45 CFR §164.522
45 CFR §164.530 (Documentation and retention)

Revision Date:
11/19/2013
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-010
Subject	Routine Uses & Disclosures	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 4

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that information of individuals served can be used and disclosed for treatment, payment, and the health care operations of the agency without obtaining a HIPAA authorization from the individual served or his/her personal representative.

PURPOSE

The purpose of this policy is to set forth the uses and disclosures that will routinely occur in TBHS which do not require a signed HIPAA authorization from the individual served or the individual's personal representative, as applicable. TBHS personnel, however, shall continue to obtain the written consent of the individual served under State law for disclosures of the individual's information made outside of TBHS. HIPAA does not change this practice.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

The HIPAA privacy rule defines these terms broadly as follows:

Health Care Operations: Is defined broadly to mean (1) conducting quality assessment and improvement activities including contacting individuals served and health care providers with information about treatment alternatives; (2) reviewing the competence or qualifications of health care professionals, evaluating provider performance, conducting training programs, credentialing, certification, and licensing activities; (3) conducting or arranging for medical review, legal services, and auditing services (including compliance reviews); (4) business planning and development; and (5) business management and general administrative activities.

Payment: Means activities undertaken by a provider to obtain reimbursement for health care services provided to the individual served. This includes, but is not limited to, activities related to coverage and eligibility determinations, billings, claims management, collections, review of services related to medical necessity or justification for charges, UR activities, and certain disclosures (e.g., name, address, DOB, account number) to reporting agencies for individuals served.

Protected Health Information: Means any health information, including graphic information of individuals served, that is created or received by a provider, and which relates to the past, present, or future physical or mental health condition of an individual served , the provision of health care to the individual or payment related to the provision of health care to the individual, and that identifies or can be reasonably used to identify an individual served. This can include the individual's entire medical record, physician orders, prescriptions and test results, scheduling logs or computerized scheduling, service activity logs, billing slips, many commonly used reports, and data appearing on computer monitors of the individual served.

Treatment: Means the provision, coordination, or management of health care and related services (including coordination and management by a provider with a third party; consultation between health care providers relating to an individual served; or referral of an individual for health care from one provider to another).

PROCEDURES

OHCA Statement

In accordance with the Pre-Paid Inpatient Health Plan (PIHP) Privacy Policy and in support of the Organized Health Care Arrangement (OHCA), it is the policy of TBHS, as related to the Health Insurance Portability and Accountability Act (HIPAA) of 1996:

- that there are uses and disclosures that could routinely occur at TBHS that do not require a signed HIPAA authorization from the individual served or the individual's personal representative, as applicable. TBHS personnel, however, shall continue to obtain the written consent of the individual served under State law for disclosures of information of the individual served made outside the agency.

- that when using and disclosing Protected Health Information (PHI) or for treatment, payment, and health care operational purposes, TBHS must make reasonable efforts to limit the amount of PHI of individuals served and Electronic Protected Health Information (EPHI) used and disclosed to that which is minimally necessary to accomplish the intended purpose of the use.

Some uses and disclosures that are considered treatment, payment, or operations and, therefore, do not require a HIPAA authorization are:

- Use of information of individuals served (including medical records from previous providers) by physicians, therapists and other staff for treatment purposes;
- Disclosure of information of individuals served to insurance companies for payment purposes;
- Use of PHI of individuals served by the internal finance staff for billing and operations; and
- Disclosure of information of individuals served to health plans for coverage determinations, eligibility determinations, medical necessity/appropriateness review, justification of charges, utilization review, pre-certification, or pre-authorization.

Although obtaining a detailed HIPAA authorization is not required for the above activities, TBHS must obtain consent from the individual served, or his or her personal representative in the following circumstances:

- Disclosure of protected health information to a provider of mental health services to the recipient.
- Agency personnel shall also obtain the individual's written consent to disclosures of information made outside of TBHS in furtherance of:
  -Treatment
  -Payment activities, or
  -Running of TBHS' health care operations

This consent is the current consent/release form used by TBHS and does not need to be a detailed HIPAA authorization form. This consent can be obtained through TBHS' usual process for obtaining consent from individuals served.

Disclosures to Another Provider for Treatment, Payment, or Operations:

In addition to uses and disclosures of PHI for TBHS' own treatment, payment or operations, the HIPAA privacy rule also allows TBHS to disclose PHI in certain cases for other providers' treatment, payment and operations as follows:

For Treatment: Disclosures may be made, as necessary, to another health care provider outside of TBHS for treatment of the consumer.

For Payment: Disclosures may be made to another health care provider or health plan, so that the other provider or plan can obtain payment for services.

For Health Care Operations: Disclosures may be made to another health care provider or health plan for the other entity's health care operations, if both TBHS and the other health care provider have a relationship with the individual served and the disclosure is for one of the following purposes:

- Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines (the primary purpose of these studies cannot be to obtain generalized knowledge, i.e., cannot be research studies disguised as QA/QI);
- Population based activities related to improving health or reducing health care costs;
- Protocol development;
- Case management and care coordination;
- Contacting providers and individuals served about treatment alternatives
- Evaluation of providers;
- Evaluation of health plan performance;
- Conducting training programs; and
- Accreditation, certification, licensing or credentialing activities

TBHS should continue to obtain written consent for these disclosures even though a HIPAA authorization is not required. Thus, TBHS personnel are responsible for obtaining the written consent of individuals served using the TBHS' current consent/release forms for any disclosures of information outside of TBHS for the purposes listed in this section.

Disclosures to Family Members/Friends Who are Not Personal Representatives:

If the individual served does not object, TBHS may disclose the individual's health information, without obtaining a HIPAA authorization, to the following persons if they are involved in the individual's healthcare or payment of health care, provided that the information is relevant to the person's involvement with the individual served (Note that if the family member or friend is the personal representative then the personal representative stands in the shoes of the individual served and this section does not apply):

- family member
- relative
- close personal friend

- other person identified by the individual served as being involved in the his/her health care or payment of health care

Although HIPAA does not require written authorization or consent as noted above, TBHS shall continue to follow its current policy to obtain written consent under State law when disclosing information of individuals served to a family member or friend who is not a personal representative of the individual served. A copy of the individual's PHI may be provided to another designated individual if the request is in writing and signed by the individual served or his or her legal representative (guardian). The release must clearly identify the designated individual and where the copy of the PHI should be sent. Accordingly, TBHS personnel shall obtain the individual's written consent/release prior to disclosing the individual's information to a friend or family member using TBHS' current consent/release forms.

Procedure for Uses and Disclosures:

1. If a use or disclosure of PHI of individuals served (excluding psychotherapy notes which are discussed in the authorization policy) is for treatment, payment or operations of the agency or of another provider or health plan subject to the conditions set forth above, there is no need to obtain a signed HIPAA authorization from the individual served. However, TBHS employees are responsible for continuing to obtain written consent with regard to disclosures of information of individuals served outside of the agency for treatment, payment and operations and for disclosures to family members. TBHS personnel shall use the current consent/release forms of TBHS and shall follow TBHS' usual process for obtaining the signatures.

2. If an employee has a question as to whether a use/disclosure is for treatment, payment, or operations, he or she is responsible for contacting the Privacy Officer.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
45 CFR §164.501 (definitions)
45 CFR §164.502 (general rules for uses and disclosures)
45 CFR §164.506 (treatment, payment, or operations)
45 CFR §164.510 (b) (disclosures to family members, etc.)
MCL 330.1748
MAC 330.7051

Revision Date:
11/19/2013
11/30/2016
10/16/2019
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-011
Subject	Uses & Disclosures Involving Authorizations	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 7

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that the uses and disclosures that do not fall within the routine uses and disclosures set forth in Routine Uses & Disclosure Policy, X-003-010 or the special circumstances set forth in HIPAA Policy, Uses & Disclosures Involving Special Circumstances, X-003-012, typically require a HIPAA authorization.

PURPOSE

The purpose of this policy is to set forth the circumstances in which a HIPAA authorization is required.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Instructional Guidance:

Providers including behavioral health providers may use and disclose PHI of individuals served in a number of circumstances that will require that the provider first obtain a HIPAA authorization from the individual prior to using or disclosing the information for that purpose. TBHS also has set forth guidelines and procedures for this process in Recipient Rights Policy, VII-001-019. In general, providers must obtain an authorization, under HIPAA, for uses and disclosures:

- related to psychotherapy notes as specifically defined by HIPAA (see subsequent topic heading); and
- falling outside of treatment, payment, and health care operations (remember the provider does not need authorization for those purposes) and falling outside any of the special circumstances categories discussed in the previous policy (e.g., disclosures required by law); and

Because of the sensitive nature of psychotherapy, the HIPAA privacy rule treats psychotherapy notes differently than other types of medical information for treatment, payment, and operations. Under the privacy rule, a provider must obtain a valid HIPAA authorization prior to using or disclosing psychotherapy notes except under the following circumstances:

- They are being used by the originator of notes for treatment;

- They are being used/disclosed by the provider for its own training program in which students and trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
- They are being used or disclosed by the provider to defend itself in a legal action or other proceedings brought by the patient; or
- They are being disclosed in certain special circumstances such as required disclosure to the Secretary of the Department of Health and Human Services in connection with a HIPAA investigation; disclosures required by law; disclosures related to health oversight activities concerning oversight related to the originator of the notes; disclosures involving averting a serious threat to a person; or disclosures about a decedent to a coroner or medical examiner.

The authorization requirement only applies to notes that are truly psychotherapy notes under HIPAA. For purposes of HIPAA, psychotherapy notes are notes recorded in any form (computer, hard-copy, tape, etc.) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the medical records of the individual served. The following are not considered psychotherapy notes: medication prescription and monitoring, counseling session start and stop times, the modalities and frequency of treatment, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date.

For many behavioral health providers, the majority of uses and disclosures occurring on a day-to-day basis will not require HIPAA authorization.

In addition to psychotherapy notes, some common examples of when a provider must obtain authorization from the individual served prior to using or disclosing information include:

- Disclosures of medical information/medical records to a disability insurance company/social security/housing authority at the request of the individual served (i.e., the individual served signs a form and the insurance company sends a request for information to the agency);
- Disclosures of medical information to an employer or school in connection with return to work or school slips;
- Disclosures of health information made to a school in connection with clearance for camp or for participation in sports and other activities;
- Disclosures related to research studies in cases where the Institutional Review Board (IRB) has not granted a waiver of the authorization requirement. Note that Michigan law under MCL 330.1748 would allow disclosure for research purposes without an authorization. However, the Agency must comply with HIPAA as it is more stringent and thus a HIPAA authorization is required; and
- Disclosures for most marketing activities (note that there are some exceptions which are discussed in more detail below)

The privacy rule requires a provider to obtain authorization in connection with using/disclosing PHI of individuals served for marketing. Marketing is broadly defined to include any communication about a product or service that encourages a person to purchase or use the product or service. As some standard and necessary communications could be interpreted as marketing under this definition, the privacy rule states that the following types of communications will not require authorization:

- Communications made to an individual served about treatment, case management, or coordination of health care, including recommendation of services, products and referrals that are important and specific to that patient's treatment. For example, a physician or other health professional may suggest a particular product or clinic that might help the individual stop smoking or the provider may send a prescription refill reminder to the individual served;
- Communications made to an individual served for his/her treatment;
- Communications made to an individual served describing entities that participate in a network or describing the types of services and products provided by the agency;
- Communications made face-to-face with the individual served at a visit such as discussions relative to and the provision of sample products ; and
- Promotional gifts of nominal value. For example, pens, magnets, calendars, mouse pads, or coffee mugs with the name of the agency, if the Agency participates in this type of activity.

Many behavioral health providers may only engage in the types of marketing activities discussed above that do not require authorization. Each agency should carefully think through (and make a checklist) whether they engage in any type of activity that could be marketing related and which does not fall within the above exceptions. These activities will require authorization.

In addition to marketing, as a general rule, a provider is required to obtain an authorization for uses and disclosures of PHI or individuals served related to research. However, authorization is not needed in the following limited circumstances:

- Authorization is not required if there is a documented waiver of authorization from an IRB or privacy board (employees should ask the privacy officer whether a waiver of authorization has been obtained in connection with the research project);
- Authorization is not required if the information is being gathered or used in preparation for research (for example, to identify potential research subjects or populations) as long as the uses and disclosures are necessary to the research and the information does not leave the provider;
- Authorization is not required for research if the individual served is deceased, the use or disclosure is solely for research and is necessary to the research.

General Requirement for Authorization:

Uses and disclosures that do not fall within the routine uses and disclosures set forth in Routine Uses & Disclosure Policy, X-003-010 or the special circumstances set forth in HIPAA Policy, Uses & Disclosures Involving Special Circumstances, X-003-012, typically require a HIPAA authorization.

Some common examples of when authorization is needed include:

- Uses and Disclosures related to psychotherapy notes as specifically defined by HIPAA (see below for exceptions);
- Disclosures made to disability insurance companies;
- Disclosures of medical information to an employer or school (for example, return to work/school slips);
- Disclosures made to a school camp or for participation in sports and other activities;
- Disclosures for research (unless an exception applies); and
- Disclosures for marketing (see below for examples of marketing and non- marketing activities)

Psychotherapy Notes:

Under the privacy rule, a provider must obtain a valid HIPAA authorization prior to using or disclosing psychotherapy notes except under the following circumstances:

- They are being used by the originator of notes for treatment;
- They are being used/disclosed by the provider for its own training program in which students and trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
- They are being used or disclosed by the provider to defend itself in a legal action or other proceedings brought by the patient; or
- They are being disclosed in certain special circumstances such as required disclosure to the Secretary of the Department of Health and Human Services in connection with a HIPAA investigation; disclosures required by law; disclosures related to health oversight activities concerning oversight related to the originator of the notes; disclosures involving averting a serious threat to a person; or disclosures about a decedent to a coroner or medical examiner.

The authorization requirement only applies to notes that are truly psychotherapy notes under HIPAA. For purposes of HIPAA, psychotherapy notes are notes recorded in any form (computer, hard-copy, tape, etc.) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical records. The following are not considered psychotherapy notes: medication prescription and monitoring, counseling session start and stop times, the modalities and frequency of treatment, results of clinical tests, and any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date.

In drafting the privacy rule, the government noted that some psychotherapists keep separate files with notes pertaining to psychotherapy sessions, which are often referred to as "process notes". These "process notes" are distinguishable from "progress notes", "the medical record" or "official records". "Process notes" capture the therapist's impressions about the patient, contain details of the psychotherapy conversation considered inappropriate for medical record and are used by the provider for future sessions. These "process notes" are often kept separate to limit access, even in an electronic record system as they contain sensitive information relevant only to the treatment provider. Importantly, these "process notes" are what the privacy rule calls "psychotherapy notes".

Any employee with questions related to whether a certain disclosure may involve psychotherapy notes should seek assistance from the Privacy Officer.

Uses and Disclosures Related to Research:

As a general rule, HIPAA authorization is required for uses and disclosures related to research. However, authorization is not needed in the following limited circumstances:

- Authorization is not required if there is a documented waiver of authorization from an Institutional Review Board (IRB) or privacy board (employees should ask the Privacy Officer whether a waiver of authorization has been obtained).

- Authorization is not required if the information is being gathered or used in preparation for research (for example, to identify potential research subjects or populations) as long as the uses and disclosures are necessary to the research and the information does not leave the Agency.
- Authorization is not required for research if the individual served is deceased, the use or disclosure is solely for research and is necessary to the research.

Uses and Disclosures Related to Marketing:

As a general rule, any communication that encourages individuals served to purchase or use certain products or services is considered marketing and requires an authorization. The following communications do not require an authorization:

- Communications made to an individual served about treatment, case management, or care coordination of health care, including recommendation of services, products and referrals that are important and specific to that individual's treatment (for example, a physician or other health professional may suggest a particular product or clinic that might help the consumer stop smoking);
- Provision of sample products during a visit; or
- Promotional gifts of nominal value (for example, pens or magnets imprinted with the name of the practice).

Authorization Contents:

To be valid, an authorization must include the following:

- A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- Name or specific identification of the person or persons who can make the requested use or disclosures;
- Name or specific identification of the person or persons who may receive the requested use or disclosures;
- A description of each purpose of the requested use or disclosure (if the request was made by the individual served and he/she does not wish to give the reason for the request, the Agency may include the words "per request of individual served" for the description).
- An expiration date or expiration event (expiration event must relate to the individual served or the purpose of the use or disclosure) (may use the statement "end of research study" if the authorization is for research). If the authorization is for the creation or maintenance of a research database or research repository no expiration date is needed and the statement "none" can be used.
- Statement of the individual's right to revoke authorization in writing, exceptions to the right to revoke, and description informing the individual served how to revoke the authorization (including a reference to the Notice of Privacy Practices).
- The consequences, if any, that will result from the refusal to sign by the individual served, including a statement that the Agency may not condition treatment on the individual's willingness to sign the authorization (subject to certain exceptions).
- Statement that information disclosed may be subject to re-disclosure by the recipient in some cases and no longer protected by the HIPAA rule.

- If the authorization is for marketing, a statement regarding any remuneration that the Agency will receive as a result of the use and/or disclosure of the individual's PHI.
- The signature of the individual served (or personal representative) and date signed.
- If signed by a personal representative, a description of the representative's authority to act on behalf of the individual.

Authorizations Cannot Be Combined:

As a general rule, an authorization cannot be combined with another type of document. (For example, an authorization cannot be combined with an informed consent). There is a limited exception for documents relating to the same research study (for example, the Agency can combine an authorization and any other form of written permission for the same study).

Two authorizations can be combined in the same document, unless one of the authorizations is for psychotherapy notes.

Treatment Cannot Be Conditioned on Authorization:

The Agency cannot require the individual served to sign an authorization as a condition for treatment unless one of the following circumstances exists:

- The authorization is for research and the treatment is related to the research OR
- The treatment is being provided for the sole purpose of creating protected health information for a third party (for example, if the Agency is contracted by an employer to conduct a mental health examination, the Agency can condition treatment on the individual signing an authorization to disclose information to the employer).

Revocation of Authorization:

An individual can revoke an authorization in writing at any time. If the Agency has already used or disclosed information in reliance upon the authorization, it will not be held accountable for disclosures made prior to the revocation.

Documentation of Authorization: All signed authorizations and revocations of authorization must be retained for at least six (6) years. If the authorization was requested for the Agency's own use, the individual served must be provided with a copy of the signed authorization.

Additional Procedures to Follow:

Please see TBHS Recipient Rights Policy, VII-001-019. In addition, the following procedures should be followed:

1. If a use or disclosure requires an authorization as set forth in this policy, the individual served should be asked to sign an Authorization form (See attached forms).
2. If the individual served brings or sends a signed authorization form in a format other than that used by the Agency, review the form to make certain that it contains all of the requirements set forth in this policy OR ask that the individual sign an authorization in the form that is used by the Agency.

3. If an individual served brings in MDHHS-5515 Standard Consent Form, TBHS is required to accept it in accordance with Public Act 129 of 2014
4. If there is a question as to whether an authorization is valid, and the individual served is unavailable or unwilling to sign the Agency's model authorization form, contact the Privacy Officer.
5. Place a copy of the signed authorization in the chart of the individual served.
6. If an individual served requests to revoke an authorization, ask for a written revocation.
7. Place one copy of the written revocation in the chart and write the words REVOKED in red ink prominently over the authorization that is being revoked.
8. If the individual's chart is in EMMIT, the authorization form must be printed, the word REVOKED written on the form (and signed and dated), then scanned back into and attached to the record. The indicator in EMMIT will be changed to revoked.
9. Take any actions necessary to stop uses and disclosures that were the subject of the authorization that has been revoked.
10. The Privacy Officer is responsible for ensuring that all Authorization forms are retained for at least six (6) years.
11. Employees with questions about whether a disclosure requires authorization should seek assistance from the Privacy Officer.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
Mental Health Code Section, 748
45 CFR §164.501 (marketing definition)
45 CFR §164.508 (authorization)
45 CFR §164.530 (documentation and retention)
TBHS Compliance Policy, X-003-010
TBHS Compliance Policy, X-003-012
Public Act 129 of 2014

Revision Date:
04/06/2010
11/19/2013
10/06/2015
11/30/2016
10/16/2019
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-012
Subject	Uses & Disclosures Involving Special Circumstances	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Susan Beals
		Page	1 of 5

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that uses and disclosures involving special circumstances (for purposes outside of treatment, payment and coordinator of care) may be made without obtaining a HIPAA authorization from the individual served.

PURPOSE

The purpose of this policy is to ensure, that due to the nature of these uses and disclosures and the need to understand the nuances of HIPAA requirements, requests for disclosures set forth in this policy should be directed to the Health Information Specialist, or designee. TBHS staff are responsible for notifying the Health Information Specialist, or designee if they receive a request for a Protected Health Information (PHI) of an individual served for any of the following circumstances. The Health Information Specialist, or designee shall handle the request.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

Uses and Disclosures Required by Law, Public Policy, or Health Oversight:

Protected Health Information may be disclosed in the following circumstances without obtaining authorization:

- The disclosure is required by law.
- The disclosure is to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability (e.g. the MDHHS).
- To report abuse, neglect, or domestic violence to an appropriate health or governmental authority,
    - Reports of child abuse are permissive even if they are not mandated by law or permission of the individual served is not obtained.
    - Reports of abuse, neglect or domestic violence for an individual served who is not a child are permitted without authorization under three circumstances:
        - where reports of suspected abuse are required by law;
        - the report is not required by law, but the individual agrees to such disclosure; or
        - the report is not required by law but is permitted by law and: (1) the provider believes (based upon professional judgment) that disclosure is necessary to prevent serious harm (to the individual served or other victims) or (2) the individual is incapacitated, a law enforcement official represents that the disclosure is not going to be used against the individual and

enforcement efforts will be materially and adversely affected if the provider waits until the individual can agree.

- Under each of these three circumstances, the individual served must be notified that the report has been made except where the provider determines, based upon professional judgment,
  that the notification would place the individual served at harm or the individual served is incapacitated and the personal representative who would receive such information on behalf of the
  individual served is the suspected abuser.

- To report adverse events, etc. to the Food and Drug Administration (FDA).
- To notify a person that he or she has been exposed to a communicable disease (if otherwise permitted by law to make this disclosure).
- To disclose information to a health oversight agency for oversight activities related to the agency as authorized by law, including:

  - Audits
  - Civil, administrative or criminal investigations, proceedings, or actions
  - Inspections
  - Licensure or disciplinary actions
  - Other oversight activities

- To disclose information to a health oversight agency for oversight activities related to the investigation of an individual served, as authorized by law and only where the investigation arises out of the receipt of health care or a claim for or qualification for public benefits related to health or where health is an issue.
- To disclose information in response to the order of a court or administrative tribunal.
- To disclose information in response to a subpoena, discovery request, or other lawful process, but only if the request is accompanied by a court-approved authorization signed by the individual served or legal representative.
- To disclose information to law enforcement officials in the following situations:

  - In compliance with a court order, court-ordered warrant, subpoena or summons issued by a judicial officer
  - In response to a grand jury subpoena
  - In response to an administrative or civil subpoena, summons or demand, provided that: (1) the information sought is relevant and material to a legitimate law enforcement inquiry; (2) the information sought is as specific and narrowly drawn as practicable; and (3) de-identified information could not reasonably have been used to meet the purpose of the request
  - Limited identifying information requested by a law enforcement official, but only the following may be disclosed:

    - Name and address
    - Date and place of birth
    - Social Security Number
    - ABO blood type and rh factor
    - Type of injury
    - Date and time of treatment
    - Date and time of death, if applicable
    - Description of distinguishing physical characteristics (including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos)

- To disclose PHI of a suspected victim to the extent required by law or, if not required by law, with the individual's consent. If consent cannot be obtained because of an emergency circumstance or incapacity and the disclosure is not required by law, disclosure may still be made under the following circumstances:

    - The law enforcement official represents that the information is needed to determine whether the individual served was a victim of a crime and the information will not be used against the individual served;
    - The law enforcement official represents that law enforcement activity will be materially and adversely affected by waiting for the victim to give consent; and
    - TBHS (in the exercise of professional judgment) determines that the disclosure will be in the best interest of the individual served.

- To disclose PHI of an individual served who has died to a law enforcement official if TBHS suspects that the individual's death was the result of criminal conduct.
- To disclose PHI to a law enforcement official related to a crime reasonably believed to have been conducted on the premises of TBHS.
- To disclose PHI of an individual served to a coroner or medical examiner as authorized by law or to a funeral director to the extent that the funeral director needs the information to provide services to the decedent.
- To disclose PHI to organ procurement agencies.
- To use or disclose PHI to avert a serious threat to health or safety including:

    - disclosure to a person who can reasonably avert, prevent or lessen the threat (including the target of the threat)
    - disclosure to law enforcement officials to identify or apprehend an individual who has made statements admitting participation in a violent crime reasonably believed to have caused physical harm to a victim or where it appears that the individual has escaped from a correctional institution or from lawful custody (unless the information regarding the commission of the crime was disclosed as a result of the individual seeking treatment to affect his or her propensity to commit the criminal conduct).

- To disclose information regarding an inmate to a correctional institution or law enforcement official having lawful custody of the inmate if the institution or official represents that the information is necessary for provision of health care to the inmate, is necessary for the health and safety of the inmate, other inmates, officials responsible for transporting the inmate, law enforcement officials, or the administration and maintenance of the safety, security and good order of the correctional institution.
- To disclose information as authorized by the worker's compensation laws.

Tracking of HIPAA Disclosures:

The HIPAA privacy rule requires that disclosures made for the reasons set forth in this policy must be tracked and provided to the individual served upon request, unless the disclosure is made for national security or to a correctional facility or law enforcement officer about an inmate.

Health oversight agencies and law enforcement officers may request that the individual's right to receive an accounting be suspended if the accounting would impede an investigation involving the individual. The request can be written or oral, but an oral request for suspension must be limited to thirty (30) days.

If an individual served requests an accounting, disclosures made during the six years prior to the individual's request must be provided (of course, disclosures made prior to the effective date of the HIPAA privacy rule need not be made available).

The accounting of disclosure must consist of the following information:

- Date of the disclosure
- Name of entity or person who received the information and address if known
- Brief description of the protected health information disclosed
- Brief statement of the purpose of the disclosure

If there are multiple disclosures to the same person or entity for the same purpose, only the first disclosure needs to be documented in the format listed above (date, name, description, purpose). All other disclosures during the time period can be summarized by providing the following:

- The frequency, periodicity, or number of disclosures made during the accounting period
- The date of the last such disclosure during the accounting period

When an individual served requests an accounting of disclosures, TBHS has sixty (60) days to provide the information. TBHS can obtain an extension of up to thirty (30) days per request by notifying the individual served of the reason for delay and the estimated completion date.

Fees:

The first accounting to the individual served during a twelve (12) month period must be provided free of charge. If the individual served requests more than one accounting of disclosures within a twelve (12) month period, TBHS can impose a reasonable cost-based charge. If a charge is imposed, the individual must be informed of the charge and given an opportunity to withdraw his or her request.

Documentation:

Information on disclosures that are subject to the accounting that is provided to the individual served must be kept for a period of at least six (6) years.

Tracking of Disclosures under MAC 330.7051 (2):

- The information released
- To whom the information is released
- The purpose claimed by the person for requesting information and a statement disclosing how the disclosed information is germane to the purpose
- The subsection of 330.1748, or other state law, under which the disclosure is made
- A statement that the receiver of the information was informed that further disclosure shall be consistent with the authorized purpose for which the information was released

Procedure for Disclosures Under Special Circumstances:

1. All requests for disclosures set forth in this policy should be referred to the Health Information Specialist, or designee to determine whether the disclosure should be made.

2. When a disclosure is made for any of the reasons set forth in this policy or for any reason set forth in MCL 330.1748, it should be documented.
3. If a consumer requests an accounting of disclosures required to be tracked under HIPAA, the Health Information Specialist, or designee must be informed of this request. The Health Information Specialist, or designee will compile the information and provide it to the individual served within sixty (60) days of the request. If the Health Information Specialist, or designee cannot meet the sixty (60) day deadline, he or she will send a letter informing the individual served of the inability to meet the deadline, the reason why, and the estimated completion date (not to exceed thirty (30) days after the initial sixty (60) day deadline).
4. If the individual served has requested an accounting of disclosures within the past twelve (12) months, the Health Information Specialist, or designee may inform the individual served that reasonable cost-based charges will be imposed, and if the individual served still wants the disclosure, the Health Information Specialist, or designee may prepare an invoice setting forth these charges and request payment at the time the disclosure is made.
5. The Health Information Specialist, or designee is required to maintain a copy of all disclosures and documentation that is provided to the individual served for at least six (6) years.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Recipient Rights Policy, VII-001-019
45 CFR §164.512 (uses and disclosures not requiring authorization)
45 CFR §164.528 (accounting of disclosures)
45 CFR §164.530 (documentation)
MCL 330.1748
MCL 330.1748a
MCL 330.1750
MCL 330.1920
MCL 330.1946
MAC 330.7051

Revision Dates:
10/06/2014
11/30/2016
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-013
Subject	Social Security Numbers	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to abide by the Michigan Social Security Number Privacy Act 454 of 2004 in all of its applications and requirements.

PURPOSE

The purpose of this policy is to ensure that TBHS has addressed the Michigan Social Security Number Privacy Act 454 of 2004 as further defined in this policy.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Not applicable.

PROCEDURES

This law went into effect on March 1, 2005. It generally prohibits the disclosure of social security numbers in certain circumstances. The law prohibits any person, including organizations, from doing the following with regard to using all or more than four (4) sequential numbers of a person's social security number:

1. Publicly displaying the numbers;
2. Using the numbers as the primary account for a person;
3. Visibly printing the numbers on ID badges or cards or membership cards, permits or licenses;
4. Requiring an individual to use or transmit the numbers over the internet or computers unless the connection is secure;
5. Requiring an individual to transmit the numbers to gain access to a website or computer network unless the connection is secure; and
6. Including the numbers in or on any document sent to an individual if the numbers are visible on or, without manipulation, from outside of the envelope or package.

In addition, as of January 1, 2006, with certain exceptions, the law prohibited including social security numbers in any document mailed to a person unless doing so is authorized by law; the document is sent as part of an application or enrollment process initiated by the person; the document is sent to establish, confirm status of, service, amend or terminate an account, contract, policy or employee health benefit; the document is mailed by a public body; or the document is mailed at the request of the person whose number appears on the document.

The person who knowingly violates the law is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $1,000 or both. A person can also bring a civil action to recover actual damages suffered as a result of a violation.

In compliance with the January 1, 2006, Michigan Social Security Number Privacy Act 454, it is the policy of TBHS that:

1. All staff will ensure, to the extent practicable, the confidentiality of social security numbers. Under no circumstances shall more than four sequential digits of a social security number be included on any document mailed outside TBHS, except as required by law, nor will it be publicly displaced in any manner.
2. Social Security numbers are not to be used as passwords or identifiers for any TBHS computer system. A social security number will not be used in the ordinary course of business except as TBHS may determine is necessary to verify a person's identity or to administer employee benefits, such as health insurance.
3. Unlawful disclosure of social security numbers is strictly prohibited.
4. Access to information or documents that contain social security numbers is limited to those staff on a need to know basis, where such information is necessary for successful completion of job duties.
5. Any documents that contain social security numbers that are no longer required by TBHS are to be shredded so as to maintain confidentiality.
6. Violations to this policy may result in disciplinary actions up to and including discharge.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Michigan Social Security Number Privacy Act 454 of 2004

Revision Dates:
09/20/2022

Policy Section	HIPAA Privacy	Policy Number	X-003-014
Subject	Breach Notification	Issue Date	04/06/2010
		Revision Date	09/20/2022
		Approved By	Susan Beals
		Page	1 of 6

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) following the discovery of a breach of unsecured Protected Health Information (PHI), that there will be a notification to each individual whose unsecured PHI was believed to have been accessed, acquired, used or disclosed.

PURPOSE

To define the process and protocols for employees to take when a known or suspected breach of confidentiality has occurred, in accordance with 45 CFR (sections 164.404, 164.406, & 164.408).

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Breach – For purposes of this policy, a breach is defined as the acquisition, access, use or disclosure of PHI in a manner that is not permitted under the Health Insurance Portability & Accountability Act (HIPAA) privacy regulations, and which compromises the security or privacy of PHI of an individual served. This means that there would be a significant risk of financial, reputational, or other harm to the individual. A breach would not be considered to pose a significant risk if the PHI at issue does not include certain identifiers. Identifiers in the Privacy Rule (45 CFR) include the following:

- Date of Birth
- Names
- Social Security Numbers
- Case Numbers
- Account Numbers
- Health Plan Numbers
- Addresses (other than town/city/state)
- Certificate/Licensure Numbers
- Vehicle Identifiers
- Telephone Numbers
- Fax Numbers
- E-mail Addresses
- Full-face and Comparable Images
- Biometric Identifiers (e.g. fingerprints)
- Internet Protocol Address Numbers
- Uniform Resource Locators (URLs)
- Device Identifiers and Serial Numbers
- Genetic Information

Encryption-Algorithms that encode plain text into non-readable form, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. 128-bit encryption is currently the standard. Encryption technology is intended to make PHI private.

Excluded Breach – For the purpose of this policy, it is not considered a breach if:

- There is an unintentional acquisition, access or use of PHI by a workforce member or person acting on behalf of TBHS, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the privacy regulations; or

- Any inadvertent disclosures by a person who is authorized to access PHI at TBHS or a business associate to another person authorized to access PHI at TBHS and the information is not further used or disclosed in a manner not permitted under the privacy regulations; or
- A disclosure of PHI where TBHS has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information; e.g. if TBHS sent a record to an incorrect individual served, the document is returned to TBHS by the post office as undeliverable and is unopened. In such a case, TBHS can conclude that the incorrect addressee could not have retained the PHI.

Note that under the regulations, TBHS retains the burden of proof to show why the matter falls under one of the above three (3) exceptions.

Genetic Information-The person's genetic tests, the genetic tests of the person's family members, the manifestation of a disease or disorder in the person's family members, or any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the person or any family member of the person.

Health Information Technology for Economic and Clinical Health (HITECH) Act – On August 24, 2009, the United States Department of Health and Human Services (HHS) began enforcing new regulations requiring health care providers, health plans, and other entities covered under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (45 CFR) to notify individuals when/if their health information is breached. These are referred to as "breach notification" regulations and were passed as part of the American Recovery and Reinvestment Act (ARRA) of 2009.

Protected Health Information (PHI) – Individually identifiable health information including demographic data, that relates to the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Unsecured PHI – PHI that is not rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of technology or methodology set forth in HHS guidance.

PROCEDURES

A. Safe Harbor from Breach Notification Reporting

1. PHI that is encrypted, or disposed of securely in accordance with TBHS Compliance Policy "Document Retention" X-001-006. Encryption is a critical tool to minimize the risk of a breach occurrence.

B. Individual Notification:

1. Following the discovery of a breach of unsecured PHI maintained by TBHS, TBHS is required to notify the applicable individuals served(or their next of kin if the individual served is deceased) whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed in the breach. This notification must occur without unreasonable delay but no later than sixty (60) calendar days following the discovery of the breach (except when

the delay is required by a law enforcement official who determines that a notification would impede a criminal investigation or cause damage to national security). The notification shall include, to the extent possible:

- A brief description of what happened, date of the breach, and date of discovery of the breach, if known;
- A description of the types of PHI involved (e.g. full name, social security number, address, diagnosis, and other types of information involved);
- Any steps that individuals should take to protect themselves from potential harm as a result of the breach;
- A brief description of what TBHS is doing to investigate the breach, mitigate harm and to protect against future breaches;
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site or postal address.

2. This notification must be given in plain language. In general, the written notification should be provided by first-class mail to the last known address of the person (unless the individual has specifically requested electronic mail). In situations where TBHS believes the possibility exists for imminent misuse of the unsecured PHI, TBHS may provide notice of the breach to affected individuals served by telephone in addition to the written notice.

3. In the case that there is insufficient or out-of-date contact information, TBHS will provide substitute notice, including, when there are ten (10) or more individuals for whom there is insufficient contact information, a conspicuous posting on the TBHS website, or a notice in a major print (such as a state or local newspaper or magazine) or using a broadcast media.

C. Media Notification:

1. In addition to notifying affected individuals of the breach, when a breach of unsecured PHI involves more than five-hundred (500) individuals served, TBHS shall provide notice to appropriate prominent media outlets serving the state or jurisdiction. This will be done without unreasonable delay following discovery of the breach (in no case later than sixty days after discovery). This would typically be in the form of a press release to appropriate media outlets serving the county/area. The information required for the notification will contain the same information as discussed above for individual notification.

D. Government Notification:

1. 500 or more individuals: For breaches of unsecured PHI involving five-hundred (500) or more individuals, TBHS shall also provide notice to the government within sixty (60) days of the breach, contemporaneously with the notifications to the individuals, in the manner specified on the HHS website. TBHS will utilize the HHS electronic report form and the reporting instructions/format specified by HHS at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

2. Less than 500 individuals: For breaches involving less than five-hundred (500) individuals, TBHS shall maintain a log using the "Breach Notification Log Form" and shall report this information to

HHS on an annual basis (no later than 60 days after the end of each calendar year). TBHS will utilize the electronic report form and the reporting instructions/format specified by HHS at:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

E. Process for Employees when a Suspected or Known Breach of Confidentiality has Occurred:

1. If any TBHS employee becomes aware of any issue or matter that could possibly impact TBHS' breach notification obligations, the employee must immediately report the information to the TBHS Compliance Officer using any of the following methods:

   - Phone reporting: Compliance Officer direct line at (989) 672-3014 or to the Compliance Hotline at (989) 672-3145
   - In writing to: Tuscola Behavioral Health Systems 323 N. State Street, Caro, MI 48723 Attn: Compliance Officer

2. Employees are not expected nor should they attempt to make a determination as to whether an actual breach (as defined in the "Definitions" section below) has taken place. Rather, employees are expected to report any known or suspected instances where PHI may have been accessed or disclosed inconsistent with the HIPAA privacy regulations and TBHS Compliance Policies "Minimum Necessary/Need to Know Protocols for Routine Disclosures to Medicaid and Other Health Plans" (X-003-003) and "Uses and Disclosures Restricted to-Minimum Necessary Information" (X-003-004). Failure to report known or suspected issues is a violation of this policy and can result in disciplinary action in accordance with TBHS' discipline/employment policies and procedures (see also TBHS Compliance Policy "Internal Reporting" X-001-003).

3. Examples of issues that should be reported for further investigation include, but are not limited to:

   - Access of data/files/records by unauthorized individuals;
   - Access of data/files/records by authorized individuals but for improper non-business purposes;
   - Disclosure of data/files/records to unauthorized individuals;
   - Disclosure of PHI without an authorization when an authorization is required; and
   - Disposing of PHI such as hardcopy reports or other paper without following appropriate destruction protocols (e.g. failure to shred reports prior to disposal) (see also TBHS Compliance Policy "Documentation Retention" X-001-006).

4. Upon receipt of a report, the Compliance Officer will conduct an investigation to determine whether TBHS has a notification obligation under the regulations. A risk analysis will be performed to determine whether PHI has been compromised.

5. The following factors shall be considered in performing a risk analysis:

   - Who impermissibly used or received the PHI.
   - The nature and the extent of the PHI involved, including types of PHI and the likelihood of re-identification.
   - Whether the covered entity has already taken immediate action to completely mitigate the risk of harm.

- Whether impermissibly disclosed PHI was returned prior to it being accessed by unauthorized individuals.

6. It is also TBHS policy and a requirement of TBHS business associate agreements that all business associates, subcontractors, or vendors must report (within forty-eight hours) any breach of confidentiality consistent with this policy.

F. Procedure for Investigating a Breach:

Upon receipt of a report or learning of an issue that may impact TBHS' breach notification obligations, the Compliance Officer and additional staff, as appropriate, shall do the following:

1. Investigate the Breach: Conduct an investigation to determine if the matter involved unsecured PHI. Legal counsel may be consulted to assist in analysis of the issues. If the matter involved unsecured PHI, the Compliance Officer, and other staff as appropriate, shall determine whether or not a breach has occurred. The following actions shall be taken by the Compliance Officer and/or other TBHS staff:

   a. Determine whether there has been an impermissible use or disclosure under the privacy regulations. The Compliance Officer shall gather and document all relevant facts and circumstances pertinent to the issue.

   b. If there has been an impermissible use or disclosure, TBHS must determine and document whether the impermissible use or disclosure compromises the security or privacy of the PHI (i.e. that it poses a significant risk of financial, reputational, or other harm to the individual). Legal counsel should be consulted at this stage.

   c. A determination must be made as to whether or not the breach is considered excluded. A breach is excluded if:

      - There is an unintentional acquisition, access, or use of PHI by a workforce member or a person acting on behalf of TBHS , if such acquisition, access or use was made in good faith and within the scope of authority and does not result in a further use or disclosure in a manner not permitted under the privacy regulations; or
      - Any inadvertent disclosures by a person who is authorized to access PHI to another person authorized to access PHI and the information is not further used or disclosed in a manner not permitted under the privacy regulations; or
      - A disclosure of PHI where TBHS has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Note: Under the regulations, TBHS retains the burden of proof to show why the matter falls under one of the above three (3) exceptions. Legal counsel should be consulted when making this determination.

Note: The Compliance Officer may consult with legal counsel as part of the process to assist in analyzing the issues and in making determinations as to appropriate reporting.

2. Report the Breach: If the results of the investigation reveal that a reportable breach has occurred, the Compliance Officer and/or other appropriate administrative staff is required to make notification without unreasonable delay but no later than sixty (60) calendar days following the discovery of the breach in accordance with items a., b., and c. above.

RELATED FORMS & MATERIALS

Breach Notification Log

REFERENCES/LEGAL AUTHORITY

45 CFR (Sections 164.404, 164.406, 164.408) @ http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

Section 105 of Title I of the Genetic Information and Nondiscrimination Act of 2008 (GINA)

NIST Computer Security Standards (Federally Approved Guidelines for Media Sanitation) @ nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-88r1.pdf

http://www.wisegeek.com/what-is-encryption.htm

TBHS Compliance Policies:

TBHS Compliance Policy, Internal Reporting, X-001-003
TBHS Compliance Policy, Document Retention, X-001-006
TBHS Compliance Policy, Minimum Necessary/Need to Know Protocols for Routine Disclosures to Medicaid & Other Health Plans, X-003-003
TBHS Compliance Policy, Uses & Disclosures Restricted to-Minimum Necessary Information, X-003-004
45 CFR Parts 160 and 164
Genetic Information Nondiscrimination Act of 2008

Revision Dates:
08/05/2011
06/01/2012
11/19/2013
10/06/2014
10/06/2015
11/30/2016
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-001
Subject	Business Associate Agreement	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) for those business associates who maintain, create or transmit Electronic Protected Health Information (EPHI) on behalf of TBHS, that the appropriate business associate security language is included in all contracts.

PURPOSE

The purpose of this policy is to ensure all contracts include language on expectations regarding security of EPHI.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Business Associate: An entity that performs functions, activities or services on the behalf of the covered entity that involves the use or disclosure of PHI.

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

1. The following security language shall be included in all contracts:

   To the extent that the Vendor creates, maintains, or transmits EPHI, the Vendor shall:

   a. Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality; integrity and availability of the EPHI that the Vendor creates, receives, maintains or transmits on behalf of TBHS, the Covered Entity, as required by the Security Standards;

   b. Ensure that any agent, including a subcontractor, to whom Vendor provides EPHI agrees to implement reasonable and appropriate safeguards to protect the EPHI;

2. Implement procedures so that any security incident involving PHI of which a vendor becomes aware is promptly reported to TBHS, the Covered Entity.
3. Subcontractors of business associates are also considered business associates if they create, receive, maintain, or transmit PHI.
4. HIPAA rules directly apply to business associates and their subcontractors, including:
   a. All applicable provisions of the Security Rule.

b. The Privacy Rule's use and disclosure limitations, including the minimum necessary and de-identification standards.
c. An accounting of disclosures of PHI.

5. Business associates and subcontractors of business associates can also be directly liable for HIPAA noncompliance and related violations.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
11/19/2013
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-002
Subject	Computer Access	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to enforce certain determinations as to which members of the workforce and other contracted individuals are authorized to access Electronic Protected Health Information (EPHI) and the types of EPHI that they may access.

PURPOSE

The purpose of this policy is to establish expectations pertaining to employee access to EPHI.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

Based on various job duties, TBHS has established which categories of employees need certain information. This analysis will be updated on a periodic basis. All members of the workforce and others given access are responsible for complying with the access levels and restrictions that apply to their positions. These individuals may only seek access to additional EPHI if granted permission by their immediate supervisor, the Chief Executive Officer or the Chief Operating Officer.

For those staff that have not been granted access to EPHI but may occasionally need access, the program supervisor shall request that the Health Information Specialist give the appropriate level of temporary access to the EPHI.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
10/06/2014
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-003
Subject	Data Backup	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS), through Technology Services, to have security measures in place that include processes for the organization's computers, networks and systems. Data back-up processes must be documented and reviewed periodically by the information and technology service provider and tested on a regular basis, the results of which are to be available to TBHS staff.

PURPOSE

The purpose of this policy is to provide information for management and workforce members performing periodic computer system backups to ensure that critical data is adequately preserved and protected against loss and destruction.

APPLICATION

This policy relates to all designated information system storage devices utilized by the TBHS organization as specified by the service level agreement for technology services.

DEFINITIONS

None

PROCEDURES

The backup will, at a minimum, include:

1. Physical Access Controls
    a. The minimum acceptable level of physical security for any backup system or server(s) is to place it behind two sets of security doors with key-code access.
    b. Physical access to backup equipment must be approved by the appropriate information technology administrator or designee.

2. Backup Schedule
    a. At a minimum, modified data on designated storage devices must be incrementally backed up at the end of each work day and a full systems backup must be performed at least once per week. Critical data should be backed up, regardless of where it resides. On a weekly basis, at least one full backup must be stored off-site in a media safe. The server farm is located at a third-party location.
    b. A process must be implemented to verify the success of the electronic information backup.
    c. Backup schedule logs:

i. The backup software should capture a list of all files and directories encountered and saved. Logs should contain information about successful backups, unsuccessful backups, backup media that was left in place accidentally and overwritten, when and where the media was sent offsite, the success or failure of restore tests and bad media encountered which may affect your ability to obtain files from a previous backup.
ii. Assign a primary band backup workforce member to rotate the media and note any problems or exceptions. Write an entry for successful backups, the date and which media was utilized. Keep the written logs with the backup storage media.

d. Legible, unique labels shall be placed on all backup media.

RELATED FORMS & MATERIALS

NIST SP 800-34 (http://csrc.nist.gov/publications), this is related material only. It cannot be inferred that all or any items detailed in the NIST document are included in this policy. It is for reference purposes only.

REFERENCES/LEGAL AUTHORITY

Administrative Safeguards – HIPAA Section 164.308(a)(7)

Revision Dates:
05/31/2012
11/19/2013
10/06/2014
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-004
Subject	Designation & Responsibilities of Security Officer	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS), as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Regulations, to designate a Security Officer.

PURPOSE

The purpose of this policy is to establish the responsibilities and functions of the Security Officer.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

Designation and Responsibilities of the Security Officer:

1. The TBHS Security Officer and/or the information technology service provider is responsible for conducting and overseeing the risk analysis and risk management process.
2. Ensure the information technology service provider and/or Information Systems Specialist for TBHS creates and maintains an inventory of all hardware, software and information systems in order to determine where Electronic Protected Health Information (EPHI) is stored, how it is transmitted, and which employees/members of the workforce currently have access to each workstation and system.
3. Ensure the information technology service provider identifies the type of information contained on each workstation or system.
4. Determine the criticality of the data, i.e., how the loss or short term unavailability of the data would impact TBHS.
5. Make good faith efforts to identify all known and/or anticipated threats to EPHI and any vulnerability that would cause a program or system to be impacted by threats.
6. When risks are identified, oversee the process to determine that the costs associated with minimizing the risks are identified.
7. Present information regarding identified risks and costs of potential solutions to the TBHS Chief Executive Officer, as the representative of the TBHS Board of Directors, so that determinations can be made based upon the risks to TBHS and the costs associated with mitigating these risks.
8. Oversee the determination of the levels of computer access, requested by program supervisors.
9. Provide security reminders.
10. Document and maintain reports of security incidents and the steps taken to mitigate such incidents.

11. Oversee the updating and testing, as deemed appropriate by the agency administration, of the information technology service provider contingency plan.
12. Oversee the periodic evaluation of the TBHS security procedures and implemented technical safeguards to determine whether TBHS is making reasonable efforts to comply with the HIPAA Security Rule.
13. Maintain any documentation related to changes in security policies or procedures.
14. Maintain documentation of the designation of Security Officer for a minimum of six (6) years from the time a designation is made.
15. Maintain the written security policies.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Regulations

Revision Date:
08/05/2011
11/19/2013
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-005
Subject	Disaster Recovery Contingency Plan	Issue Date	09/29/2008
		Revision Date	09/17/2018
		Approved By	Sharon Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to have a Disaster Recovery Contingency Plan in place.

PURPOSE

The purpose of this policy is to provide information for management and workforce members to ensure recovery from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing individually identifiable protected health information.

APPLICATION

This policy relates to all computer information technology utilized by the network/information technology service provider and other organizations, including TBHS, as specified by the service level agreement for technology services.

DEFINITIONS

Not applicable.

PROCEDURES

The Disaster Recovery Plan is documented in the Contingency Plan of the network/information technology service provider. The disaster recovery plan should also be reviewed periodically by the network/information technology service provider and all changes are approved by the TBHS CEO.

The TBHS Electronic Health Record (EHR) System Recovery Plan provides guidance for responding to system failures and other unexpected outages of the electronic health record. The EHR Recovery Plan shall be reviewed annually or as needed by the Information Systems Specialist and all changes will be approved by the TBHS CEO. Should an actual system failure or outage occur, the plan will be reviewed and revised to address any practical application issues.

RELATED FORMS & MATERIALS

TBHS Compliance Policy X-004-003
TBHS Electronic Health Record System Recovery Plan

REFERENCES/LEGAL AUTHORITY

Administrative Safeguards - HIPAA Section 164.308(a)(7)

Revision Date:
08/05/2011
11/19/2013
10/06/2014
11/30/2016
09/17/2018

Policy Section	HIPAA Security	Policy Number	X-004-006
Subject	Electronic Device Use	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that all laptop computers, tablets and any other devices or applications containing electronic protected health information (EPHI), that are accessible outside of TBHS be kept in a secure manner that does not allow access to unauthorized individuals or risk of exposure of EPHI.

PURPOSE

The purpose of this policy is to ensure that the TBHS devices and applications containing EPHI are appropriately secured.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

The following procedures shall be followed at TBHS:

- All devices and applications containing EPHI that are accessible outside of TBHS must have perimeter security and access control with a firewall, password protection and other security measures.

- All TBHS employees who seek to use devices and applications containing EPHI that are accessible outside of TBHS must have approval of their immediate supervisor for use in this manner. TBHS employees utilizing such devices and applications may temporarily save data to the workstation, provided the data is removed and saved to a network location as soon as possible. Temporarily saving data to an encrypted flash drive is allowed. However, data should be removed from the flash drive as soon as possible and saved on a network location, as appropriate.

- All TBHS employees who seek to use devices and applications containing EPHI that are accessible outside of TBHS locations shall be in compliance with the Management Information Systems Policy – Safeguards – Remote Computing - XI-002-007.

- "Hard copy" (paper) protected health information transports shall be kept to a minimum for use outside of TBHS locations. All documents containing PHI will be returned promptly to TBHS for scanning or disposal.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Management of Information Systems Policies, Safeguards XI-002-001 through XI-002-009.

Revision Date:
08/05/2011
11/19/2013
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-007
Subject	E-Mailing of Protected Health Information	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Susan Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that Electronic Protected Health Information (EPHI) may only be e-mailed in accordance with the criteria and rules set forth by TBHS.

PURPOSE

The purpose of this policy is to ensure that standards for the transmission of EPHI are observed.

APPLICATION

This policy shall be applicable to staff of all TBHS Programs, direct and contracted.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

The procedural rules include:

1. Consumer EPHI may be e-mailed within TBHS when necessary to perform a job task and only if the information meets "need-to-know" status.

2. Consumer EPHI may only be emailed outside of TBHS if:

   - The e-mail is in connection with the performance of a necessary task (example, an e-mail to a third-party payer in connection with the payment of a billed claim);
   - The recipient of the e-mail has a need to know the information;
   - PHI is not contained in the title of the e-mail; and
   - The e-mail is sent accompanied by a confidentiality statement.
   - The e-mail has been encrypted using an accepted encryption tool/process.

TBHS, or their designee, may monitor e-mail systems for improper EPHI disclosures. No user shall have the expectation of privacy in anything they store, send or receive on the TBHS e-mail system. TBHS may monitor messages without prior notice, however, TBHS is not obligated to monitor e-mail messages.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

TBHS Management of Information Systems Policies, E-Mail, XI-002-008

Revision Date:
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-008
Subject	Emergency Mode Operations Plan	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to maintain an Emergency Mode Operations Plan.

PURPOSE

The purpose of this policy is to provide information for management and workforce members to ensure that access to critical electronic protected health information (EPHI) is maintained during an emergency situation.

APPLICATION

This policy shall apply to staff of all TBHS Programs, and contracted providers and the computer networks and systems that affect care of individuals served. Computers, networks or systems that are not used for care of individuals served do not fall under this policy.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

During an emergency situation emergency access measures must be implemented. This includes access to a computer, computer network or electronic system of the TBHS organization that contains EPHI. This is allowed in the event of an emergency, if denial to that information could inhibit or negatively affect necessary care to the individual served. Every effort must be made to ensure that access to the system is available in case of emergency.

The network/information technology services provider shall be responsible for the enforcement of this policy.

RELATED FORMS & MATERIALS

TBHS Compliance Policy X-004-003

REFERENCES/LEGAL AUTHORITY

Administrative Safeguards - HIPAA Section 164.308(a)(7)

Revision Date:
08/05/2011
11/19/2013
10/06/2014
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-009
Subject	Firewalls	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that all systems and applications containing electronic protected health information (EPHI), that are accessible outside of TBHS must have perimeter security and access control using a firewall.

PURPOSE

The purpose of this policy is to ensure that the TBHS systems and applications containing EPHI are appropriately secured.

APPLICATION

This policy applies to all computers, computer networks and systems that affect TBHS care of individuals served. Computers, networks or systems that are not used for care of individuals served do not fall under this policy.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

The following procedures shall be followed at TBHS:

- All systems and applications containing EPHI that are accessible outside of TBHS must have perimeter security and access control using a firewall.
- Firewalls must be configured to support the following minimum requirements:
  - Limit network access to only authorized workforce members and entities;
  - Limit network access to only legitimate or established connections (an established connection is return traffic in response to an application request submitted from within the secure network);
  - Console and other management ports must be appropriately secured or disabled;
  - Mechanisms must be present to log failed access attempts; and
  - Servers and other devices containing firewalls must be located in a physically secure environment allowing access to only necessary users (i.e., those people that must have access).
- The configuration of firewalls used to protect networks containing EPHI-based systems and applications is documented and reviewed periodically by the TBHS information technology service

provider. Security documentation will be provided as needed to the TBHS Security Officer. This documentation should include information that outlines and explains the firewall configuration.

RELATED FORMS & MATERIALS

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
10/06/2014
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-010
Subject	General Rules to Safeguard TBHS Computer Network	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharm Beals
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that all employees are responsible for following general rules that are intended to safeguard both the integrity and availability of the TBHS computer network.

PURPOSE

The purpose of this policy is intended to safeguard both the integrity and availability of the TBHS computer network.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

As a condition to receiving access to computer systems, individuals are responsible for complying with the following general guidelines in addition to other requirements set forth in the TBHS Management Information Systems Policies.

General Rules:

The following general rules are intended to supplement, and not replace, the TBHS Management Information Systems Policies. In the event of a conflict between the TBHS Management Information Systems Policies and the HIPAA Security Policies with respect to EPHI, the HIPAA Security Policy shall govern. TBHS' Management Information Policies include:

Information Systems & Technology Use

- Role of the information technology services provider
- Computer System Usage
- E-Mail
- Computer Hardware
- Computer Software
- System Access & Passwords
- Data on Workstations
- Remote Computing
- Email
- System Backup

- Texting & Email Messaging

Communications & Devices

- Individuals may be assigned a TBHS cellular telephone and/or pager.
- Individuals with access to voice mail should ensure the voice mailbox does not become full and inaccessible to outside entities.
- Individuals are not permitted to add or download software programs to tablets, laptops or workstations without first submitting this in the form of a request to the Information Systems Specialist. This includes, but is not limited to, downloading free multimedia programs, games and instant messaging applications. Adding unauthorized software may decrease system performance and has the potential to cause the introduction of viruses into the TBHS system.
- Individuals are not permitted to download EPHI to a disk, flash drive or CD unless this is needed to carry out a necessary job function. The flash drive shall also be of the encrypted variety.
- Individuals are not permitted to open attachments associated with personal e-mail (for example, jokes, video clips, etc.) since these types of attachments are often used as a mechanism to spread viruses and other malicious software.
- Individuals are not permitted to open e-mail attachments from persons/entities they do not know (e.g., individuals may not open attachments ending in "exe." As such attachments may contain viruses).
- Individuals are expected to alert the Information Systems Specialist if they receive suspicious e-mails.
- Individuals who receive e-mails warning of new virus threats should forward such e-mails to the Information Systems Specialist to determine whether the threat is realistic or a hoax.
- Individuals are not permitted to disable anti-virus software installed on their tablet, laptop or workstation.
- Individuals are responsible for notifying the Information Systems Specialist if they are unable to login to a program or if they receive an unusual error message when trying to login.
- If individuals have portable devices such as tablets or laptops at home or in the community, these devices must be kept in a secure manner so others cannot access or see EPHI. TBHS staff shall also not save any EPHI to the device's local storage media, e.g. local hard drive (with the exception of the flash drives as noted above).
- To the extent reasonable, those individuals with tablets, laptops or workstations in areas where visitors and others may see the screen, shall ensure the screen is turned to minimize unauthorized viewing or utilize a screen filter.
- Individuals should be cautious when eating or drinking around or near tablets, laptops or workstations.
- Individuals should log-off tablets, laptops and workstations when leaving them unattended for any significant period of time.
- Individuals may not move, remove or install hardware or software to a computer without getting authorization from the Information Systems Specialist.
- Individuals are responsible for reporting security incidents to the Security Officer and the Information Systems Specialist.

RELATED FORMS & MATERIALS

None

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-011
Subject	Monitoring	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to monitor its compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations.

PURPOSE

The purpose of this policy is intended to establish a process whereby the TBHS Security Officer, with assistance from the information technology services provider and the Information Systems Specialist, will be responsible for periodically evaluating TBHS to determine whether TBHS is making reasonable efforts to comply with the HIPAA Security Rule.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

Periodic Evaluations

The Security Officer, with assistance from the information technology services provider and the Information Systems Specialist will perform or oversee evaluations that are completed of the TBHS Security policies and procedures and safeguards at intervals deemed appropriate by the Security Officer but no less than annually.

Other Reviews

In addition to the Periodic Evaluation, TBHS may also conduct an evaluation upon certain triggering events, including:

- Changes in the HIPAA security regulations that would impact policies and procedures of TBHS;
- Changes in the technology environment of TBHS

The TBHS Security Officer shall maintain documentation of such reviews.

Information System Activity Review/Reports

- In an effort to monitor the security of TBHS electronic protected health information (EPHI), the information technology services provider, as requested by the TBHS CEO and COO, have the capability of running various reports to detect activity such as login attempts, misdirected e-mails and virus activity. A schedule will be maintained.

RELATED FORMS & MATERIALS

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-012
Subject	Physical Security	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shaun Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to protect the confidentiality, integrity and availability of electronic protected health information (EPHI) in the agency.

PURPOSE

The purpose of this policy is intended to ensure the security and confidentiality of EPHI.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

TBHS has enacted a number of physical security measures. They include:

Physical Access to Facilities Containing EPHI

TBHS has a number of physical locations containing EPHI. As part of its physical security measures, the following procedures are in place limiting access to TBHS facilities:

1. Only certain authorized individuals are given keys and/or keypad and alarm codes for entry into TBHS buildings during non-working hours when the building entrances are locked.

2. During work hours, all visitors are required to check in by signing visitor logs and receiving a visitor's tag to be worn in a visible location for the duration of time that they are in a TBHS building. Visitors are not allowed to merely wander through any TBHS building unaccompanied; as required, all visitors must be escorted by TBHS staff.

3. TBHS staff members who are visiting another TBHS building are required to wear their TBHS identification badge or receive a visitor badge from the building receptionist.

Maintenance Records

The TBHS Security Officer, or designee, is responsible for overseeing that repairs and modifications to the physical components of the TBHS buildings that are related to security are documented on a Maintenance Log.

Moving of Work Stations

Documentation of movement of computer hardware throughout TBHS is maintained. It is the responsibility of the Information Systems Specialist to move equipment and to keep an inventory of location of equipment. It should be noted that data is largely stored on the servers, except in the cases where individual personal computers (PCs) or laptops are in use. Those utilizing the virtual desktop interface or VDI environment are not at risk as data is all stored on the servers.

Hardware/Software Destruction

The following procedures are undertaken in the event that disposal of systems containing EPHI is required:

- All disks, tapes, CDs and other media that may contain EPHI should be destroyed or erased prior to disposal;
- The information technology services provider is responsible for the disposal of hard drives and shall determine the best manner in which to destroy or erase EPHI; and
- Prior to erasing any hard drive, a duplicate copy should be made of any EPHI that the Information Systems Specialist or other TBHS Administrative Staff determines should be retained. Again, with the data being stored mostly on the servers due to the implementation of the virtual desktop interface or VDI environment, this is becoming an obsolete measure. As a result, TBHS staff shall not save EPHI to any hard drive internally located on any computer or other memory device being used for the purpose of the utilization of EPHI.

RELATED FORMS & MATERIALS

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
10/06/2015
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-013
Subject	Remote Access	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that the TBHS Chief Executive Officer (CEO), or designee, must approve any users seeking to remotely access (via, fiber, broadband, T1, DSL, ADSL line, etc.) entry to the TBHS network.

PURPOSE

The purpose of this policy is to ensure the security and confidentiality of Electronic Protected Health Information (EPHI) and the network.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

As a condition to receiving remote access to computer systems, individuals are responsible for complying with requirements set forth in the TBHS existing Management Information Systems Policies.

It is the responsibility of all users with remote access privileges to ensure that the connection to the network is not used by unauthorized individuals. Any users who are granted remote access privileges must remain constantly aware that the connections between their location and TBHS are literal extensions of the TBHS network, and that they provide a potential path to TBHS sensitive information, including EPHI.

All remote access users must take every reasonable measure to protect the network and EPHI.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Management Information Systems Policy

Revision Dates:
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-014
Subject	Reporting of Security Incidents-Mitigation of Harm	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) and the information technology services provider that all members of the workforce are responsible for reporting any security incidents of which they become aware to the Information Systems Specialist or the TBHS Security Officer.

PURPOSE

The purpose of this policy is to appropriately handle security incidents and prevent reoccurrences.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

Identification and Reporting of Security Incidents

A security incident is defined as the "attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system."

Examples of security incidents that should be reported, include, without limitation:

- Passwords that have been lost, stolen, shared or used by persons other than the individual to whom the password was assigned;
- Introduction or potential introduction of viruses, worms, Trojan horses, malware or other malicious software into the computer systems;
- Unauthorized access to networks, computer systems, or facilities/equipment rooms housing the computer systems;
- Unauthorized introduction of software by a member of the workforce;
- Misdirection of email containing EPHI; and
- Improper/unauthorized destruction of EPHI.

TBHS employees who are aware of a security incident are required to report to the Information Systems Specialist or the Security Officer by any of the following methods:

- In-person report;

- Telephone; or
- Written communication sent to the attention of the Information Systems Specialist or the TBHS Security Officer.

Documentation and Investigation of Security Incident and Response

Upon receipt of a report of a security incident or potential incident, the Security Officer shall investigate the matter. Depending on the nature of the incident, information technology service provider staff and/or the TBHS Security Officer may consult with TBHS legal counsel to direct and assist in the investigation. Upon looking into the matter, if a security breach has been confirmed, the TBHS Security Officer is responsible for documenting the matter including the outcome of the investigation and the response to the security breach. This information shall be kept by the Security Officer in a folder marked "CONFIDENTIAL". If the investigation was directed by legal counsel, the Security Officer should mark the folder "CONFIDENTIAL AND SUBJECT TO THE ATTORNEY/CLIENT PRIVILEGE." The Security Officer is responsible for documenting on a Security Incident Form.

Mitigation of Harm

The information technology service provider staff and/or the TBHS Security Officer has the responsibility to make a determination regarding the steps that should be taken, if any, to mitigate harm as a result of a confirmed security breach. If the incident involves a major wrongful disclosure of information of individuals served, the network/information technology services provider and/or the TBHS Security Officer is responsible for making a recommendation to the TBHS Chief Executive Officer regarding what steps should be taken to mitigate the harmful effects of the breach. In such cases, the information technology service provider staff and/or the TBHS Security Officer should not take action without consulting with the TBHS Chief Executive Officer. The network/information technology service provider staff and/or the TBHS Security Officer may consult with others in the field or expert consultants in addressing potential mitigation options and, depending on the severity of the issue, should coordinate with the TBHS CEO and TBHS legal counsel with regard to the matter prior to making any final recommendations or taking any actions.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
10/06/2014
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-015
Subject	Sanctions	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Sharon Beals
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that individuals will be sanctioned for breaching security policies and procedures.

PURPOSE

The purpose of this policy is intended to appropriately handle the breach of security policies and procedures to prevent reoccurrences of preventable problems and mitigate any harm.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

The TBHS Security Officer and/or designee shall work in coordination with the TBHS Human Resources Department by informing them of the violation. In imposing sanctions, TBHS may consider the severity of the violation, whether the violation was intentional or unintentional and whether the violation indicates a pattern or practice of improper use or disclosure of EPHI. Sanctions may include, but will not be limited to:

1) a verbal warning;
2) a written reprimand;
3) the cost of re-education;
4) suspension; and/or
5) termination.

This Sanction Policy, however, does not alter the at-will status of employees.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision:
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-016
Subject	Change of Employment Status	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that when an individual ceases employment, otherwise ceases providing services at TBHS or experiences a change in status with TBHS (e.g., through termination, resignation, retirement, suspension, leave of absence), steps will be taken as soon as possible, to modify or stop rights to access electronic protected health information (EPHI).

PURPOSE

The purpose of this policy is to discontinue access to EPHI, as appropriate.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

The following measures will be taken, as appropriate to the situation:

- Decrease the individual's ability to access EPHI (such as making adjustments to the type(s) of EPHI that the individual should have access to depending on their new status);
- The Information Systems Specialist and Health Information Specialist and/or the information technology service provider shall address the following:
  - The individual's password to all agency computer systems and networks will be disabled or deleted including access to the EHR;
  - All remote access will be terminated;
- Access to external sites that contain EPHI not a part of overall access to the information system shall be disabled or deleted upon notification from the Human Resources Department.

  Depending on the change of status, the individual will be asked to return all keys, keycards, laptops, cell phones, name badge and any other equipment (termination, resignation, retirement, suspension and possibly leave of absence); and
- The individual may undergo an exit interview that includes a discussion of the confidentiality of PHI including EPHI (if appropriate).

- If applicable, the return of all items listed above will be required before a final paycheck is given to the individual.

- The Security Officer is responsible for providing a procedure to ensure that the Human Resources Department and the Information Systems Specialist have systems in place to ensure timely coordination so that access to EPHI is promptly terminated upon a change of employment status.

RELATED FORMS & MATERIALS

TBHS Termination Check List
TBHS Exit Interview Form

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-017
Subject	User Names and Passwords	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Susan Beals
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS), through the information technology service provider to assign each member of the workforce a unique user name and a password or passwords that represent adequate security to the entire TBHS computer network.

PURPOSE

The purpose of this policy is intended to maintain secure access to the network that contains electronic protected healthcare information.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

Management of user names and passwords:

Assigned user names **may not** be changed without the approval and assistance of the Information Systems Specialist.

Passwords are used for a variety of purposes. Some of the more common uses include: user level accounts, e-mail accounts, voicemail passwords, etc. Everyone should be aware of how to select strong passwords. **No two passwords used by any individual may be identical.** This means that if you use one password to login to a tablet, laptop or workstation, that same password cannot be used to exit a screen saver, access voicemail, etc. Users should also avoid selecting passwords to access TBHS systems that are identical to passwords used to access non-agency systems (e.g., Hotmail accounts, Internet sites etc.) If someone gains access to any of a user's passwords, that person should not be able to exploit that password to gain access to other accounts or systems.

Passwords are a critical aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire TBHS network. As such, all users (including contractors and vendors with access to the TBHS systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

To ensure that all passwords used to control access to any network, system, application, and electronic media or file containing electronic protected health information (EPHI) are secure and not easily predicted, the following procedures should be adhered to:

- Passwords must be a minimum of at least eight (8) characters in length.
- Passwords must incorporate at least one letter and at least one number.
- If passwords are case-sensitive, they must contain at least one upper case and one lower case letter.
- Passwords must not include easily guessed information such as personal information, names, pets, birthdates, etc. nor may passwords consist of such words spelled backwards or preceded or followed by a number.
- Passwords should not be words found in a dictionary.
- Passwords shall be changed at least every six (6) months.
- Passwords must not be inserted into e-mail messages or other forms of electronic communication.
- Passwords must not be written down near any workstation or stored on any workstation.
- Workforce members must not use the "remember password" feature in Microsoft Internet Explorer, Outlook, Firefox, Chrome, Eudora, etc. Computers must be configured to require password entry for each access event.

If there is a part of the TBHS system that does not support the minimum structure and complexity as detailed in the aforementioned guidelines, one of the following procedures must be implemented:

- The password must be adequately complex to ensure that it is not easily predicted; or
- If an alternative password structure must be implemented, the complexity of the chosen alternative must be defined and documented.

RELATED FORMS & MATERIALS

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Dates:
08/05/2011
06/01/2012
11/19/2013
10/06/2014
11/30/2016
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-018
Subject	Virus & Other Malicious Software Management	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) and the information technology service provider that processes be established and maintained to monitor and react to the potential threat from malicious software, including the risk of viruses, worms, Trojan horses, malware, spy ware and other types of system intrusions. Further, it is policy that every TBHS workstation should have anti-virus software installed.

PURPOSE

The purpose of this policy is to ensure that the network security and integrity is not compromised due to introduction of a virus or other malicious software.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the TBHS network.

DEFINITIONS

Electronic Protected Health Information (EPHI): Contains individually identifiable information which is transmitted by electronic media and/or maintained in electronic media.

PROCEDURES

As part of the TBHS efforts to protect the security and integrity of EPHI, all users are required to comply with the following guidelines:

- Never open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your deleted items folder.
- Delete spam, chain and other junk e-mail without forwarding it.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.

The network/information technology service provider will monitor the threat and/or the effect of malicious software. This topic will be discussed in the information technology service provider setting. System information that supports this subject will be reviewed at that time. The performance of any technology services aimed to combat malicious software will be reviewed for the accuracy of its operations and to verify the use of current versions. Information related to relevant findings will be sent to the TBHS Security Officer or designee.

RELATED FORMS & MATERIALS

REFERENCES/LEGAL AUTHORITY

Not applicable.

Revision Date:
08/05/2011
11/19/2013
10/06/2014
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-019
Subject	Wireless Access	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	
		Page	1 of 2

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that employees accessing TBHS networks via wireless communication mechanisms obtain approval from the TBHS Chief Executive Officer (CEO), or designee and adhere to strict guidelines for use.

PURPOSE

The purpose of this policy is to ensure that network security and integrity is not compromised.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the TBHS network.

DEFINITIONS

Local Area Network (LAN): A communications network that serves users within a confined geographical area.

Media Access Control Address (MAC): The unique serial number burned into Ethernet and Token Ring adapters that identifies that network card from all others.

PROCEDURES

Guidelines regarding wireless systems:

Only wireless systems that meet the criteria of this policy are approved for connectivity to TBHS networks. This policy applies to all wireless data communication devices (e.g., personal computers, cellular telephones, etc.) connected to any TBHS internal networks, including any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to TBHS networks do not fall under the purview of this policy.

All wireless access points connected to the TBHS network must be registered and approved by the information technology services provider. These access points are subject to periodic penetration tests and audits. All wireless network interface cards (i.e., PC cards) used in laptop or desktop computers must be registered with the information technology services provider.

All wireless LAN access must use vendor products and security configurations approved in advance by the information technology services provider.

Wireless implementations must maintain point-to-point hardware encryption of at least 128 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC

address. All implementations must support and employ strong user authentication, which checks against an external database.

RELATED FORMS & MATERIALS

REFERENCES/LEGAL AUTHORITY

Source for definitions: PCMAG.com
TBHS MIS Policy XI-002-006, Wireless Access

Revision Date:
08/05/2011
11/19/2013
10/06/2015
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-020
Subject	Workforce Clearance	Issue Date	09/29/2008
		Revision Date	09/20/2022
		Approved By	Shawn Brake
		Page	1 of 1

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) to identify workforce clearance criteria and procedures for workforce members who will be given access to electronic protected health information (EPHI) as part of their job duties.

PURPOSE

The purpose of this policy is to ensure that the appropriate staff is provided with appropriate level(s) of network access in order to perform their job duties.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, that have authorized access to the TBHS network.

DEFINITIONS

Not applicable.

PROCEDURES

Although the HIPAA Security Rule does not mandate the specific measures that must be taken, TBHS has identified the following measures as appropriate:

- The individual will be asked if they have ever been disciplined for breaching security at a previous job or facility;
- The individual will need to meet the requirements imposed by Public Acts 27, 28 and 29 of 2006.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

2006 Michigan Public Acts 27, 28 and 29

Revision:
09/17/2018
09/20/2022

Policy Section	HIPAA Security	Policy Number	X-004-021
Subject	Electronic Signatures	Issue Date	10/06/2014
		Revision Date	09/20/2022
		Approved By	Susan Beals
		Page	1 of 3

POLICY

It is the policy of Tuscola Behavioral Health Systems (TBHS) that electronic signature is used for the electronic health record as a means of attestation of electronic entries, transcribed documents, and computer-generated documents.

PURPOSE

The purpose of this policy is to establish a foundation for facilitation of the use of electronic signatures for the electronic health record generated during healthcare operations, validate information accuracy and completeness, and to verify the identification and appropriateness of electronic health record authors.

APPLICATION

This policy shall apply to staff of all TBHS Programs, direct and contracted, as well as individuals served that have been sanctioned to legally sign an agency document, either by requirement or as a matter of the course of agency business.

DEFINITIONS

Attestation: the act of applying an electronic signature to the electronic health record (EHR) content, showing authorship and legal responsibility for a particular unit of information.
Authentication: the security process of verifying a user's identity with the system that authorizes the individual to access the system (i.e., the sign-on process). Authentication shows authorship and assigns responsibility for an act, event, condition, opinion, or diagnosis.
Authorship: attributing the origination or creation of a particular unit of information to a specific individual or entity acting at a particular time.
Electronic signature (e-signature): a generic, technology-neutral term for the various ways that an electronic record can be signed, including a digitized image of a signature, a name typed at the end of an email message by the sender, a biometric identifier, a secret code or PIN, or a digital signature.
Signature log: a typed listing of the provider(s) identifying their name with a corresponding handwritten signature.

PROCEDURES

Properly executed electronic signatures are considered legally binding as a means to identify the author of electronic health record entries, confirm content accuracy and completeness as intended by the author, and to ensure e-signature integrity is maintained for the life of the electronic health record. The electronic signature process operates within a secured infrastructure (i.e. network), ensuring integrity of process and minimizing risk of unauthorized activity in the design, use, and access of the electronic health record.

An electronic signature serves three main purposes:

- **Intent:** an electronic signature is a symbol that signifies intent such as an approval of terms, confirmation that the signer reviewed and approved the content, or the signer authored the document and approves the content.
- **Identity:** the signature identifies the person signing.
- **Integrity:** a signature guards the integrity of the document against repudiation (the signer claiming the entry is invalid) or alteration.

All TBHS-authorized EHR users assigned with the ability to sign into and use the electronic health record shall never share their unique login credentials (login ID and password) with others.

The individual whose name is on the signature bears the responsibility for the authenticity of the information being attested.

The information systems network, related software products, and the EHR shall include protections against e-signature modification.

Verification of content accuracy and completeness of each entry or document is made by the author prior to attestation.

An e-signature event captures and displays the e-signature, author's name, credentials, date, and time of application.

Once an entry has been electronically signed, the system shall prevent deletion or alteration of the entry and its related electronic signature for the life of the referenced documentation.

Updates to electronic health record information made after finalization (or the signature event/attestation) will be handled as an amendment, correction or augmentation.

Documents requiring an individual served, legal representative, or witness signature are part of the legal electronic health record of the individual served. Approaches to signatures of individuals served, , legal representatives, or witnesses may include electronic signatures such as digitized handwritten signature and digital signature. The same principles for uninterrupted security and guarantee of unalterable functionality apply.

Where appropriate, a signature log may be kept. A signature log may be used to establish signature identity as needed throughout the electronic health record documentation.

RELATED FORMS & MATERIALS

Not applicable.

REFERENCES/LEGAL AUTHORITY

CMS "Medicare Program Integrity Manual" (Pub. 100-08), Chapter 3, Section 3.3.2.4.B.

"Electronic Signature, Attestation, and Authorship. Appendix A: HL7 EHR-System Records Management and Evidentiary Support (RM-ES) Functional Profile Standard Excerpt." *Journal of AHIMA* 80, no.11 (November-December 2009)

Revision Dates:
11/30/2016
09/17/2018
09/20/2022