METHODONE DISASTER RECOVERY SUMMARY INFORMATION SHEET

Disaster recovery of your Computalogic software system is achieved using MethodOne.

MethodOne is a web-based software solution for Methadone Maintenance Facilities. The system is housed in a secure data center located in Pittsburgh, Pennsylvania. There are multiple servers in the event of an unplanned outage, data from the MAT program can be brought up on another server, typically within hours. In addition to this failover policy the system backs up QBH's data nightly and stores the data at a completely different data center halfway across the country. In the event of a catastrophic event that would cause outages at QBH's physical location and Computalogic's data center, QBH's system and data would be up and running in approximately 24 hours.

In the event of a power outage at Computalogic's physical location they recommend having back-up power like a generator or battery backups for QBH's modem, router, key computers (i.e., nursing computers, dispensing pumps, label printers, etc.). At a minimum QBH should have a laptop with a fully charged battery on hand so that MethodOne can be accessed for scheduling and medication reports.

. In the event the Internet also fails at a QBH location, an additional path for fail over should be maintained. It is recommended that QBH acquire a wireless access point from Verizon or AT&T, choosing based on which offers better service in QBH service areas. They usually have prepaid ones or ones that are billed monthly. At a minimum, a mobile phone should be kept operational that is capable of setting up and sharing a mobile hotspot with acceptable service.

Once all these items are in place it is highly recommended that QBH plan to test the equipment during, or in conjunction with, fire drills to ensure that the equipment is working. This will ensure that the staff knows where all the items are and how to use them in the event of an outage. It is highly recommended that, where batteries are involved, good records be kept as to when they were purchased and the frequency of when the tests are performed.

Computalogic, LLC

USING ABBREVIATIONS

- All staff, when using abbreviations and symbols while documenting in medical records, must use only those authorized by this Company. Likewise, they must never use those listed in the prohibited (DO NOT USE) list.
- Staff requesting additions or changes to the list will submit their request to the Chief Executive Officer for consideration by the Clinical Committee.
- The abbreviations and symbols authorized are listed in Appendix A.
- The abbreviations and symbols that are prohibited (DONOT USE) are listed in Appendix B.
- Compliance with this policy is monitored on an ongoing basis. Noncompliance is reviewed and appropriate measures are taken to achieve improvement.
- All staff is trained at hire and provided annual review on abbreviations and symbols that may and may not be used. The abbreviations and prohibited abbreviations lists are provided to staff during training and are readily accessible at each office and in the QBH MAT Manual.

EVALUATION

- The Medical Records staff will review this policy annually (12 MONTHS +/- 30 DAYS) and make modifications as needed based upon changes in regulations, changes necessary due to nature of services, etc. Any revisions will be submitted to the Clinical Committee as scheduled.

FORMS

Abbreviation List
Do Not Use Abbreviation List

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONSUMER'S RIGHT OF ACCESS TO PROTECTED HEALTH INFORMATION**

RIGHT OF ACCESS OF PHI

- Consumers have the right to inspect and receive a copy their PHI maintained in a designated record set, except:
    - Psychotherapy notes.
    - Information prepared by QBH in reasonable anticipation of, or for use in, a civil, criminal, or administrative action.

REQUESTS FOR ACCESS TO PHI

- All requests to inspect and/or receive a copy of a consumer's PHI shall be in writing, by the consumer or the consumer's legal representative, on a Release of Information Form. The request is provided to the Medical Records staff.
    - Any disagreement or discrepancy noted by the consumer/guardian may be rebutted in writing and will be attached to the medical record.
- The Medical Records staff shall review the request and deem whether the form is valid and HIPAA compliant.
- The request will be forwarded to the Medical Director. The Medical Director will determine if the requested information may be released; if it is determined that some part of the information is to be withheld the Medical Director will document why this determination has been made. The Medical Director or designee will oversee the consumer's review of the record; the Medical Director may be asked to participate if the primary concerns are medical in nature.
    - In no case will any information be released to a psychiatric consumer or guardian without prior approval from either the Clinical Director or Medical Director.
    - If the Clinical Director or Medical Director has documented in the consumer's record that it would be contraindicated to have the consumer view their record, the consumer will be informed that they may appeal the decision to the Recipient Rights Officer if they choose (refer to Recipient Rights Policy).
- QBH must act upon the request to access PHI no later than 30 days after receipt of the request.
- If QBH is unable to comply with the timeframe of the 30 days allowed, QBH may extend the time for acting on the request by no more than 30 days provided that, within the time QBH was required to act, QBH provided the consumer with a written statement of the reasons for the delay and the date by which QBH will act on the request. QBH may extend the time to act on a specific request to access PHI only once.

Initiated: 1/2022
Reviewed/Revised: 1/2023, 1/2024, 1/2025

APPROVAL OF REQUESTS FOR ACCESS TO PHI

- If the request to access the consumer's PHI is approved, the consumer or their legal representative must be informed of the approval and provide access as follows:
    - Access must be provided as requested, including the opportunity to inspect and have copied the requested PHI.
    - Access to PHI must be provided in the form or format requested if the PHI is readily producible in such form or format. If not readily producible in such form or format, it will be provided in a readable hard copy form or other format, or form, agreed upon by QBH and the consumer or the consumer's legal representative.
    - The consumer or the consumer's legal representative may be provided with a summery or explanation of the PHI requested in lieu of providing access to the PHI, if the consumer or the consumer's legal representative agrees in advance to receive such summary or explanation, and to the fees, if any, charged by QBH for the summary or explanation.
- A convenient time and place must be arranged for the consumer or the consumer's legal representative to inspect and, if requested, have the PHI documents copied for them. The copy of the PHI may be mailed, as requested by the consumer or the consumer's legal representative. The consumer or the consumer's legal representative may not inspect the medical record without the presence of QBH personnel.

REVIEW BY THE CONSUMER

- The consumer/guardian will at no time be left alone to view the medical record.
    - A nurse who is familiar with the consumer should sit with the consumer during record review to provide any needed clarification. This staff member shall notify the consumer and schedule the review.
    - Any incomplete record must be brought current prior to the review.
    - The staff member sitting with the consumer for record review will instruct the consumer that no alteration or removal of any part of the document is allowed and will monitor for compliance with this directive.

RECEIPT OF COPY BY THE CONSUMER

- The consumer may not take the original record or its contents. The consumer's record remains the property of QBH. Copies of the consumer's medical record will be provided when authorized. The consumer will be charged per page for copies according to the rate current at the time, subject to change by QBH at any time.

- ONLY the Medical Records staff may copy and release the record to the consumer/ guardian. If the consumer/guardian requests a copy of the record electronically, a processing fee will be charged according to the rate current at that time.

DENIAL OF REQUESTS FOR ACCESS TO PHI

- A consumer or a consumer's legal representative may deny access to the consumer's PHI only if one of the grounds for denial outlined in the section on "Unreviewable Grounds for Denial" or in the section on "Reviewable Grounds for Denial" applies.

- If a consumer's or a consumer's legal representative's request to access the consumer's PHI is denied, QBH must provide the requestor with a denial written in plain language and containing the basis for the denial.

    - If applicable, the consumer or their representative is given a statement of the consumer's rights to review the denial, including a description of how the consumer may exercise such rights, and a description of how the consumer may file a complaint with the Secretary of DHHS or with QBH. The name or title, and telephone number of QBH's Privacy Officer will also be provided.

- If QBH denies requested access to PHI, QBH shall, to the extent possible, provide the consumer or the consumer's legal representative access to any other PHI requested, after excluding the PHI to which QBH has grounds to deny access.

UNREVIEWABLE GROUNDS FOR DENIAL

- QBH may deny a consumer's or a consumer's legal representative's requests to access the consumer's PHI, without providing the consumer or the consumer's personal representative with an opportunity to seek review of the denial, in the following circumstances:

    - The consumer or the consumer's legal representative requests PHI to which there is no right of access as described in the section entitled "Right of Access to PHI."

    - QBH, acting under the direction of a correctional facility, denies an inmate's request to copy PHI, if obtaining the PHI would jeopardize the health, safety, security, custody, or rehabilitation of the consumer or other inmates, or the safety of any officers, staff, or other person at the correctional facility or involved in transporting the inmate. (Please note that if an inmate requests to inspect PHI, the request must be granted unless one or more of the other grounds for denial applies.)

    - The PHI was obtained from someone other than a healthcare provider under a promise of confidentiality, and the access request is reasonably likely to reveal the source of the PHI.

REVIEWABLE GROUNDS FOR DENIAL

- QBH may deny a consumer or consumer's personal representative access to the consumer's PHI if the consumer or consumer's legal representative is given a right to have the denial reviewed, in the following circumstances:
    - A licensed healthcare professional (e.g., physician, Clinical Director) has determined in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the consumer or of another person.
    - The requested PHI refers to another person (other than a healthcare provider), and a licensed healthcare professional has determined in the exercise of professional judgment that the access requested is reasonably likely to cause substantial harm to such person.
    - The request for access to PHI is made by the consumer's legal representative, and a licensed healthcare professional has determined in the exercise of professional judgment that the provision of access to the legal representative is reasonably likely to cause substantial harm to the consumer or to another person.

PROCESS FOR REVIEW OF DENIAL

- The consumer or personal representative shall submit to the Privacy Officer a written request to review the denial.
- The Privacy Officer shall promptly refer the request to the licensed healthcare professional who is designated by QBH to act as a reviewing official and who did not participate in the original decision to deny access to PHI.
- The designated reviewing official shall determine, within a reasonable period of time, whether or not to deny access to PHI (based on whether a "reviewable ground for denial" applies) and notify the Privacy Officer of the decision, in writing.
- The Privacy Officer shall promptly notify, in writing, the consumer or the consumer's legal representative of the designated reviewing official's determination.
- If the designated reviewing official overturns the original denial and grants access to PHI, the consumer or the consumer's legal representative will be provided access to the PHI, as described in this policy.

COPYING AND FEES

- If a consumer or consumer's personal representative requests a copy of the consumer's PHI or agrees to receive a summary or explanation of the PHI, QBH may charge the consumer or consumer's legal representative a reasonable cost-based fee, which includes only the cost of:
    - Copying, including the cost of supplies for and labor of copying;

- Postage, if the consumer or the consumer's legal representative requests that the copies or summary/explanation of PHI be mailed to the consumer or the consumer's legal representative.

- Preparation of an explanation of summary of the PHI, as agreed to in advance by QBH and the consumer or the consumer's legal representative.

DOCUMENTATION

- QBH is required to document and retain for six (6) years from the date of creation, as applicable, the following:

  - The designated record sets subject to access by consumer or consumer's legal representative, and

  - The titles of persons or offices responsible for receiving and processing requests to access the PHI.

EVALUATION

- This policy will be reviewed by the Privacy Officer annually (every 12 months +/- 30 days) and revisions made when necessary. The Policy will be forwarded to the Clinical Committee for review and approval when revisions are made and at a minimum of yearly.

FORMS

QBH MAT Consumer Medical Record Policy

GENERAL GUIDELINES

(See also the Technology Plan and Information Management Policy)

QBH licenses the use of computer software from a variety of sources. Such software is normally copyrighted by the software developer and, unless expressly authorized to do so, the Company has no right to make copies of the software except for backup and archival purposes.

When the need for increased computer memory and speed are identified, the Company upgrades existing computers whenever possible.

The Company will establish regular computer downtime to complete system backups. Unplanned downtime occurs due to lengthy electrical storms or hardware failure.

SOFTWARE MANAGEMENT

- It is the policy of the Company to respect all computer software copyrights and to adhere to the terms of all software licenses to which the Company is a party.

DUPLICATION OF SOFTWARE

- Company staff may not duplicate any licensed software or related documentation for use either on Company premises or elsewhere unless the Company is expressly authorized to do so by the agreement with the licenser. Unauthorized duplication of software may subject staff and/or the Company to both civil and criminal penalties under the United States Copyright Act.

- Staff may not give software to any individuals including consumers, staff members, and others.

- All software purchase requests need to be approved by the CEO or designee(s) for compatibility, cost, and inventory purposes.

- Software will be installed by the designee(s) assigned by the CEO. Manuals, tutorials, and other user materials shall be provided to the user. A copy of the applicable licensure agreement shall be stored with the original discs in a storage area.

- Company computers and related electronic media are Company-owned assets and must be kept both software legal and virus free. Only software purchased through procedures outlined above may be used on Company machines. Staff is not permitted to bring software from home for installation on Company electronic media without authorization from the CEO or designee(s).

- The installation of Company-owned software on home computers or other personal electronic media, or any other non-Company owned computer or other electronic media is expressly prohibited and subject to disciplinary action, up to and including termination.

- It is the policy of the Company to not allow the use of shareware unless specifically authorized by the CEO or designee(s).

- According to the U.S. Copyright Law, illegal reproduction of software is subject to civil damages of as much as $250,000 per title infringed, and criminal penalties, including fines and imprisonment of up to five years. Any Company staff that make, acquire, or use unauthorized copies of software shall be disciplined as appropriate under the circumstances, up to and including dismissal. The Company does not condone the illegal duplication of software and will not tolerate it.

ELECTRONIC MEDIA USE

- Electronic media may not be used for knowingly transmitting, retrieving or storage of communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene or X-rated communications, or are of a derogatory or threatening nature, or for "chain letters", or for any other purpose illegal or against Company policy or contrary to the Company's interests.

- Electronic media and services are primarily for the Company's business use. Limited, personal or incidental use of electronic media (sending or receiving) for personal, non-Company purposes, where authorized, is acceptable as is the case with personal phone calls. However, staff needs to demonstrate a sense of responsibility so as to not abuse the privilege.

- The Company reserves the right, at its discretion, to review a staff's electronic e-mail messages and usage to the extent necessary to oversee that electronic media services are being used in compliance with the law and with this and other Company policies. Staff should therefore not assume electronic communications are private and confidential and should transmit highly sensitive information in other ways.

- Staff that uses any security measures on a Company supplied PC, laptop, tablet or other electronic media must coordinate with the Medical Records Coordinator to establish passwords or other security devices used to access his/her files.

- No e-mail or other electronic communication may be sent which attempts to hide the identity of the sender or represent the sender as someone else, or from another Company.

- See also the Electronic Communications Policy.

UPGRADE OF COMPUTERS AND OTHER ELECTRONIC MEDIA

- When a computer system or related electronic media becomes unable to perform the tasks for which it is intended, the CEO will be notified.

    - Subject to approval from the CEO, the system will be upgraded to the needed performance level.

- If the system is too old to be upgraded to the needed level, the system may be replaced.

- Obsolete computer systems or related electronic media that have been replaced will be traded in to the supplier if they have monetary value, or properly disposed of.
  - All information shall be deleted from the hard drive(s) before trade or disposal by the IT Consultant.
  - Any pertinent information is transferred by the IT Consultant to a new computer or related electronic media before the hard drive is wiped clean.

BACK-UP

- See the Contingency Plan Policy for a description of back –up procedures and related security measures. All computers or related electronic media, programs or networks that contain confidential consumer, staff or administrative content must be backed up daily at the end of the workday (or maintained in Dropbox or other cloud storage) and, for some programs with servers, back up is at night. Back-ups of confidential data not fed to a server, but rather by a thumb drive that is password protected and encrypted are to be immediately verified and stored in a lockable fireproof box which is stored in a secure location in each office or department, or a secure offsite location known to the Human Resources Manager, if authorized by the CEO or designee. The network-based closed Electronic Medical Record is backed up daily after business hours. (See also the Technology Plan and Information Management Policy.)

UNPLANNED DOWNTIME

- Unplanned downtime occurs due to hardware failure or extended electrical power failures.

- All servers have individual uninterrupted power supplies to maintain power in the event of a power outage.
  - If the power is not restored within 5 minutes, the servers will be powered down until normal power is restored.
  - Individual workstations are to remain off until normal power is restored.

HARDWARE FAILURE

- Affected staff is to notify their supervisor or the CEO who will notify the Security Officer.

- If parts are available for the specific need, the IT Consultant will swap out the failed part.
  - If the part is not available, it will be ordered immediately, and affected staff is advised as to what electronic media to use in the interim.

- If the repair involves a server, every attempt will be made to make repairs within 24 hours.

- For the closed, network-based EMR see their Contingency Plan, Emergency Operations Mode Plan and Disaster Recovery Plan and the Technology Plan and Information Management Policy.

EVALUATION

- This policy will be reviewed and, as needed, revised, annually (12 months +/-30 days) by the Privacy and Security Officers and, as needed, the IT Consultant, with submission to the Clinical Committee for approval of needed revisions.

FORMS

Method One Software Recovery Information Sheet

QUALITY BEHAVIORAL HEALTH, INC. MAT ADMIMISTRATIVE RECORD MANAGEMENT POLICY

DEFINITIONS

Company Administrative Records: Includes, but not exclusively, financial reports, personnel and privileging files, policies and procedures, and minutes of Board and committee meetings, internal and external audit reports, quality and safety related documents.

Authorized Staff: Those designated by their respective department head to retain, retrieve or dispose of records related to their department.

Computerized Record: Any record stored in a local computer, portable disk, network server, computer disk drives, or other electronic media.

Disposal: the process by which records are disposed of after no longer needed and/or after the designated period of time.

Meeting Records: Minutes documenting the events occurring in Company meetings, i.e. Board meetings and Clinical Committee meetings.

Paper Record: Any hand-written, typed, printed or copied document.

Personnel and Privileging Records: Any record maintained by the Human Resources Department.

Record Archival: Removing records from the main network server disk drive and storing them on a disk drive specifically designated for infrequently accessed records.

Retention: Appropriate placement of records in a secure environment with limited access by authorized personnel.

Retrieval: The process by which records are accessed by authorized personnel.

ADMINISTRATIVE RECORDS MANAGEMENT

- Requesting or disclosing of confidential information is carried out in accordance with applicable state and federal statutes.
- All QBH records (computerized and paper) are retained in designated locations that are secure and limit access to authorized personnel only.
- Personnel and privileging records shall be retained pursuant to the requirements of applicable state and federal statutes and Joint Commission (JC)standards.
- Retrieval of Company records (computerized and paper) is limited to authorized personnel.
- Disposal of Company records (computerized and paper) will occur after a determined period of time as described by state and federal regulations.

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. MAT ADMIMISTRATIVE RECORD MANAGEMENT POLICY

RETENTION OF ACTIVE COMPANY ADMINISTRATIVE PAPER RECORDS

- Active personnel and privileging records are retained in Human Resources and are monitored and maintained by the Human Resources Manager.
- Active meeting records are retained in the CEO's office and are monitored and maintained by the CEO or designee.
- Financial records are retained in the offices of the Billing/Accounting Department and maintained by the Accountant.
- Quality system information is retained in Human Resources and is maintained by the Quality Management Coordinator.
- Safety system information is retained in Human Resources and is maintained by the HR Manager.

RETENTION OF INACTIVE ADMINISTRATIVE PAPER RECORDS

- Inactive personnel and privileging records are retained in the Human Resources Department for a period of one (1) year, and then they are scanned to a web-based storage. Inactive records are kept perpetually.
    - Inactive staff health related records are retained for a minimum period of thirty (30) years as required by OSHA standards.
- Financial records are retained within the Billing Department or web-based storage.
- Meeting minutes, quality and safety records shall be retained for a minimum of three years, or longer if so, required by regulatory agencies.
- Internal and external audit results, policies and procedures, and related reports are retained perpetually.

RETRIEVAL OF ACTIVE COMPANY ADMINISTRATIVE PAPER RECORDS

- Personnel and privileging records are retrieved only by designated Human Resources Department staff. Quality and safety records are retrieved by the Quality Management Coordinator and Safety Officer or HR Manager.
- Meeting minutes and related documents, policies and procedures, internal and external audit reports, and related documents are retrieved only by the CEO, or designee.
- Financial records and reports are retrieved only by designated staff within the Billing/Accounting Department.

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

RETRIEVAL OF CLOSED/INACTIVE ADMINISTRATIVE PAPER RECORDS

- Inactive records are retrieved in the same fashion as active Company records as referenced above.

DISPOSAL OF EXPIRED ADMINISTRATIVE PAPER RECORDS

- Administrative records shall be disposed of by shredding when no longer needed based upon the expiration of required retention time for the type of record.

RETENTION OF COMPUTERIZED ADMINISTRATIVE RECORDS

- Computerized administrative records are stored on the Company computer network or, in some cases on a web-based network. Computerized documents have a scheduled daily or weekly back-up process.

RETRIEVAL OR COMPUTERIZED RECORDS

- Computerized records retained on the Company network server and/or web-based network can only be retrieved by personnel with appropriate access rights.
- Access rights are defined by user-specific IDs and passwords and/or specific network server permissions limiting records retrieval only to those with proper access rights.
- Access to each category of information is defined by job title or function.

DISPOSAL OF COMPUTERIZED RECORDS

- Computerized records are archived rather than disposed of.
- When computerized records no longer need to be accessed on a frequent basis, they are removed from the main network server disk drive and stored on a media specifically designated for the archiving of records.

EVALUATION

- The Security/Privacy Officers will review this policy annually (every twelve months or once a year plus or minus thirty days) and make modifications as needed based upon changes in regulations, changes necessary due to nature of services, etc. Any revisions will be submitted to the Clinical Committee for approval.

FORMS

All administrative records/forms

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. AND DISCLOSURES **MAT BUSINESS ASSOCIATES-HIPAA USES**

POLICY

To oversee that Quality Behavioral Health, Inc., obtains satisfactory assurance from its business associates that they appropriately safeguard all individually identifiable health information/ protected health information (PHI) created, maintained, or received on behalf of Quality Behavioral Health, Inc. (QBH)

DEFINITIONS

Business Associate: means a person who, on behalf of QBH, but other than in the capacity of the workforce, performs, or assists in the performance of: 1) A function or activity involving the use or disclosure of PHI, including claims processing or administration, utilization review, quality assurance, billing management, practice management, and repricing; or 2) Any other function or activity regulated by HIPAA subpart 160.103; or 3) Provides, other than in the capacity of a member of the workforce of QBH, legal actuarial, accounting, consulting, data aggregation, or financial services to or for QBH, or to or for an organized health care organization in which QBH participates, where the provision of the services involves the disclosure of PHI from QBH or the organized health care arrangement, or from another business associate of QBH or arrangement, to the consumer.

Workforce: means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for QBH, is under the direct control of QBH, whether or not they are paid by QBH.

BUSINESS ASSOCIATE AGREEMENTS

- QBH documents the satisfactory assurances that its business associates appropriately safeguard PHI created or received on behalf of QBH through a written agreement or other legal agreement or arrangement that meets the criteria described in paragraph B.2 of this policy.

- An agreement between QBH and a business associate must:

    - Establish the permitted and required uses and disclosures of such information by the business associate. The agreement may not authorize the business associate to use or further disclose the information except that:

        - The agreement may permit the business associate to use and disclose PHI for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate; and
        - The agreement may permit the business associate to provide data aggregation services relating to the health care operations of QBH.

    - Provide that the business associate must:

        - Not use or further disclose the information other than as permitted or required by the agreement or as required by law;

- Use appropriate safeguards to prevent use or disclosure of the information not provided for by its agreement;
- Report to QBH any use or disclosure of the information not provided for by its agreement of which it becomes aware;
- Ensure that any agents, including a subcontractor, whom it provides PHI received from, or created or received by the business associate on behalf of, QBH, agree to the same restrictions and conditions that apply to the business associate with respect to such information;
- Make available PHI in accordance with a consumer's right to access PHI as described in QBH Policy;
- Make available for amendment and incorporate any amendments to PHI in accordance with QBH Policy;
- Make available the information required to provide an accounting of disclosures in accordance with QBH Policy;
- Make its internal practices, books and records relating to the use and disclosure of PHI received from, or created by the business associate on behalf of QBH available to the Secretary of Health and Human Services for the purposes of determining QBH's compliance with provisions of the Health Insurance Portability and Accountability Act (HIPPA); and
- At termination of the agreement, if feasible, return or destroy all PHI received from, or created by the business associate on behalf of QBH that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information feasible.
- Authorize termination of the agreement by QBH, if QBH determines that the business associate has violated a material term of the agreement.

OTHER ARRANGEMENTS

- The agreement or other arrangement between QBH and the business associate may permit the business associate to disclose the information received by the business associate for the purposes of proper management, administration, and to carry out legal responsibilities if:
  - The disclosure is required by law; or
  - The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidential and used or further disclosed

only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

- If a business associate is required by law to perform a function or activity on behalf of QBH or to provide any service described to QBH, QBH may disclose PHI to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this policy, provided that QBH attempts, in good faith, to obtain satisfactory assurances of safeguards to the disclosed PHI, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

EXCEPTIONS

- These procedures do not apply to the following:
  - With respect to disclosures by QBH to a health care provider concerning the treatment of a consumer;
  - With respect to disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, to the extent that the minimum necessary requirements for health plans apply and are met;
  - With respect to uses or disclosures by a health plan that is a government program providing public benefits, if eligibility for, or enrollment in, the health plan is determined by an agency other than the agency administering the health plan, or if the PHI used to determine enrollment or eligibility in the health plan, and such activity is authorized by law, with respect to the collection and sharing PHI for the performance of such functions by the health plan and the agency administering the plan.

COMPLIANCE

- QBH is out or compliance with federal requirements under – HIPAA if QBH knew of a pattern of activity or practice or the business associate that constituted a material breach or violation of the business associate's obligation under the agreement or other arrangement, unless QBH took reasonable steps to cure the breach or to end the violation, as applicable, and, if such steps were unsuccessful:
  - Terminated the agreement or arrangement, if feasible; or
  - If termination is not feasible, reported the problem to the Secretary of the Health and Human Services.

EVALUATION

This policy shall be evaluated at least annually (every 12 months +/- 30 days) and as needed by the Security and Privacy Officers based upon findings from testing or actual implementation of the plan. It shall be submitted to the Clinical Committee for approval.

Initiated: 1/2022
Reviewed/Revised: 1/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC.
AND DISCLOSURES

MAT BUSINESS ASSOCIATES-HIPAA USES

FORMS:
Business Associate Agreement

Initiated: 1/2022
Reviewed/Revised: 1/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONFIDENTIALITY, SECURTY AND INTEGRITY OF INFORMATION**

QBH establishes guidelines which provide for compliance with applicable rules and regulations as determined by the Michigan Department of Health Services (MDHS), the Joint Commission (JC) standards, Federal Department of Health and Human Services (HHS) such as the Health Insurance Portability and Accountability Act (HIPAA), HITECH, Title 42 CFR Part 2, legal principles as set for by court cases such as Tarasoff, any state mental health and privilege laws, and as may be stipulated by various funding entities. (See also the Technology Plan and Information Management Policy.)

DEFINITIONS

Confidential Information: any information protected by law with respect to who has access to the information. Confidential information includes, but not exclusively: consumer-related information, quality data, staff records, and business records. Consumer information covered by HIPAA includes any health information, including genetic information; individual identifiable health information (IIHI); protected health information (PHI/ePHI); psychotherapy notes; other consumer related records and routine notes.

Confidentiality: the safekeeping of data and information, including keeping the establishment or existence of a clinical relationship, as restricted to individuals who have need, reason, and permission for access to such data and information. This applies regardless of the format (oral, paper or electronic) with which the data and information is maintained.

Authorization for Release of Information Form: a form the consumer or legally responsible party signs which gives written consent or permission for the release of specific information and states the specific time when the release expires. Authorization or permission is different from informed consent.

De-Identified Information: health or personal information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

Privileged Information: confidential information that would otherwise be admissible in a judicial proceeding that is withheld if it is so classified. Either a consumer/guardian or the health professional may automatically claim or invoke privilege; however, this right is not an absolute as there are times when a health professional has a right, rather than an obligation, to reveal information and waive privilege and/or it may be waived in certain legally defined situations (these exceptions are usually state defined).

Sensitive Information: information that is not confidential but is deemed by QBH to be sensitive in nature and in need of protection from unauthorized personnel.

Unauthorized Personnel: any person, whether or not a staff of QBH, who does not have need, reason and permission to access confidential or sensitive information.

Protected Health Information (PHI): individually identifiable health information (IIHI), including whether an individual is in treatment, or has died, that can be used to identify and individual, that is:

- Orally communicated.
- In hard copy format such as the traditional medical record;
- Transmitted by electronic media (ePHI);
- Maintained in any mode of electronic transmission, including the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using any type of storage media;
- Transmitted or maintained in any other form or medium.
- Protected health information does not include:
    - Education records covered by the Family Educational Rights;
    - Educational records, files, documents, and other materials which contain information directly related to a student and which are maintained by an educational Company or institution or by a person acting for such Company or institution; and
    - Employment/contract records held by the QBH in its role as an employer/contractor.

Privacy is the right of the individual to decide how much, to whom, when and in what manner personal information can be shared with others. Privacy is an essential ethical principle of mental health professionals, as well as a standard of care.

Use means sharing, employment, application, utilization, examination, or analysis of PHI/ePHI by the health professional or Company that maintains the PHI/ePHI. Use includes uses within QBH.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PHI/ePHI by the health professional or outside of QBH holding the information. In some cases disclosure does not require prior authorization by the consumer/guardian; in most cases such written authorization is required.

Minimum Necessary Rule means when performing a task, only disclose the minimum amount of PHI/ePHI necessary. This rule applies to all with access to any element of PHI/ePHI but does not apply to the PHI/ePHI exchanged between treatment providers.

- ***NOTE: DO NOT ASSUME THAT OTHERS WILL REPORT OR FIX A PRIVACY OR SECURITY ISSUE. IF YOU ARE AWARE OF A PROBLEM BE RESPONSIBLE TO INFORM THE PRIVACY OR SECURITY OFFICER AND/OR OTHER RESOURCE AS SPECIFIED IN THIS POLICY IMMEDIATELY.***

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONFIDENTIALITY, SECURTY AND INTEGRITY OF INFORMATION**

- QBH shall safeguard all business related and PHI/ePHI records and information against loss, destruction, tampering, and unauthorized access or use. Consumer information is considered private if you learn about it through your job. All staff shall abide by privacy practices by securing confidential information in all locations and via all media.

- All confidential information, including oral information regarding a consumer, including consumer and staff records and any electronic information related to consumers, staff or Company business, will be protected to the extent mandated by applicable law. Consumers in the MAT program have the right to confidentiality in accordance with federal regulations (42 CFR).

- Any disclosure of consumer information, written, electronic, or verbal, shall be made only with the consumer's, or their guardian's, written authorization, or as required by law or regulation.

- QBH adheres to the requirements for the retention and disposal of consumer and staff records as outlined by State and Federal law, and JC standards. PHI information no longer is required to follow HIPAA regulations after 50 years past the death of the person.

- Computerized and other electronic information systems will have security features enabled and used to the extent necessary to facilitate confidentiality, security and integrity of information.

- Other electronic systems such as facsimile, phone, IPad, email or texting shall comply with Company confidentiality policy and regulations.

- Use of social interaction sites such as Facebook or Twitter shall not be used to communicate Company, consumer, or staff information; nor shall Company owned phones or computers be used to connect to such sites at any time. Staff may not communicate with current or former consumers using these social interaction networks.

- Posters or notices listing security reminders are posted in all critical areas and all workstations. Additionally, staff is periodically retrained on PHI/ePHI security measures and responsibilities.

- Violations of confidentiality and security by a staff member are grounds for discipline up to and including immediate dismissal.

- A Privacy Officer shall be assigned to oversee and monitor all oral and paper security as directed by HIPAA. Likewise, a Security Officer shall be assigned to oversee and monitor all electronic security.

PRIVACY SAFEGUARDS

CONSUMER RELATED CONVERSATIONS

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONFIDENTIALITY, SECURTY AND INTEGRITY OF INFORMATION**

- Conversations involving consumer PHI/IIHI should not occur where they can easily be overheard. Whenever possible hold these conversations behind closed doors, in a softer than normal voice, and in rooms with white noise equipment. Discussion of consumer treatment or other PHI outside of appropriate settings (various types of therapy sessions, treatment planning and staffing, etc.) should be avoided.

- Avoid use of names or other identifying information in conversations whenever possible. Never use a last name.

- If possible, designate a "quiet area" away from public areas to use when sensitive information exchanges are necessary.

- When it cannot be avoided and sensitive discussion must occur in a public area, the discussion should be conducted as quietly as possible and as far away from others as possible.

- Telephone conversations involving PHI should be conducted where they cannot be overheard if possible; be especially sensitive of voice volume, particularly if using a cell phone (studies show people normally speak louder when talking on a cell phone). Use a land line whenever possible. Identifying information (IIHI) should never be used in a cell phone conversation.

- Obtain instructions from the consumer/guardian about how to reach them by phone, including how to leave messages and follow those instructions to the best of your ability. If the person you are trying to reach is unavailable, only leave your name (first or last, whichever the consumer/ guardian is most familiar with) and a callback number on the answering machine or voicemail system, or with any other person that answers.

- When discussing PHI/IIHI with a consumer/guardian, or about a consumer /guardian to a third party, the other person's identity should always be confirmed before proceeding. When in doubt, you can ask for identifying information, including a callback number, and take a moment to verify the caller's identity to the best of your ability.

- If you are checking messages on your answering machine or voicemail, make sure the volume is low so that the incoming messages cannot be overheard when left or played back. If using voicemail, protect your password and change in periodically.

- Use conventional postal service mail, when possible, for communications with consumers/guardians. It is slower, but generally more secure. Document when and how communication is accomplished in the consumer record.

CONFIDENTIALITY OF PHI ON PAPER AND VISUAL CONFIDENTIALITY MEASURES

- All consumer records, regardless of format, are the property of QBH and will be maintained to serve consumers and health providers.

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONFIDENTIALITY, SECURTY AND INTEGRITY OF INFORMATION**

- The information contained in the consumer record belongs to the consumer; therefore, the consumer is entitled to have this information protected. All consumer information shall be regarded as confidential and made available only in accordance with the Release of Information section in this policy and other Company HIPAA related policies.

- A staff shall not read the consumer record of a consumer just because that consumer is a friend, relative or VIP; such action would be a breach of staff's conflict of interest obligation.

- Paper consumer records may NOT be removed from QBH, and electronic consumer records may not be transmitted or printed at any time except for Company business, or by court order or statute. As part of a court ordered Title 36 hearing, original paper records and/or electronic records are taken to and from court by authorized QBH staff for physician/ staff review during testimony. Records or other sensitive information removed for Company facilities must be kept in locked containers designated for record transport; if in electronic format, the information must be encrypted and password protected, and in the possession of QBH's provider at all times. Any release, regardless of format, must be authorized by the Medical Records staff.

    - Paper records that are removed are logged as out by Medical Records and/or Nursing Department staff and include the date removed and the date returned. These records should be returned when not in use and no later than the end of the day checked out. They are re-filed in secure cabinets or drawers upon return.

- Staff members having access to consumer records, regardless of format, and the Medical Records staff, are required to abide by the confidentiality standards of this and other HIPAA related policies. Staff shall sign an affidavit of their intent to abide by such standards at the beginning of their employment/contract.

- QBH staff is responsible for limiting access to confidential information, in whatever format, through the following measures:

    - Confidential and sensitive information at the Reception Area (i.e., sign-in sheets, computer screens, etc.) and in the Nurses' Station must be covered or blocked from view of unauthorized personnel or have security screens.

    - Record storage and computer workstations must be locked when not occupied by an authorized staff. Only authorized staff has access to the record storage.

    - File cabinets or drawers containing confidential or sensitive information will be locked when vulnerable to unauthorized personnel. Unfiled material is stored so that it is not visible and in a secure area.

    - Keys and/or keypad codes to record storage, staff desks/offices, and other locked areas will only be assigned to authorized staff.

        - ✓ Authorized staff is responsible for protecting the areas to which they have been assigned keys or informed of key codes.

- Incoming faxes will be retrieved by a designated staff and distributed directly to the intended recipient. The fax machine shall be located in a restricted area away from public or consumer access or viewing. When possible, only send to known locations where physical security of the receiving machine can be assured. Double check before sending that the proper recipient is keyed in. Make sure all faxes contain the confidentiality notice requesting faxes sent to an incorrect destination be destroyed and requesting notification to the sender of such errors

- Documents containing PHI are not to be left unattended on computer printers, photocopiers, or fax machines. This equipment is to be located in a secure location.

- Incoming mail will be date stamped and promptly forwarded to the intended recipient. Outgoing mail will be placed in a bin in the office of the staff member responsible for mailings and away from public viewing.

- Interoffice mail must be sent in approved envelopes and marked confidential if they contain PHI/IIHI. Mail routing and receptacle areas must be in a secure location away from access by unauthorized persons. If sent by mail, the material must be sent by the most secure means available and be traceable.

- Posters, wall boards, etc. with consumer names and/or pictures of consumers should not be located in unsecure or public areas. Sign in sheets shall contain only a consumer's first name and last initial and are to be blocked out or otherwise covered or removed promptly by responsible office staff. Likewise, artwork of consumers that is put on a wall shall not have the name reflected on the front of the artwork; a first name only may be written on the back of the artwork.

- Sensitive written documents that are no longer needed are to be shredded immediately or placed in an appropriate secured container for secure disposal in the near future; shredding should occur on a frequent, regular basis. Such containers should not be located in places where unauthorized persons can gain access. Trash receptacles shall not be used for disposal of un-shredded PHI at any time.

- Staff's children and spouses may not accompany and/or visit them inside Company offices (staff may go outside the office to pick up whatever a staff's spouse or child may bring by).

    - Any breaches in oral, visual and/or paper PHI compliance should be reported immediately to the Privacy Officer. The Privacy Officer shall promptly investigate the situation notify the Chief Executive Officer.

SECURITY: PHYSICAL SAFEGUARDS

INFORMATION TECHNOLOGY/SECURITY OF ELECTRONIC MEDIA

Building Access Controls

- All buildings/offices are secured with locks (and in some cases, also sensors) on all doors that require either a key, magnetic coded card, or use of a keypad for access. Only authorized staff has access to keys, magnetic cards, and/or keypad codes. Should a staff leave and/or be terminated with failure to reclaim a key, the door(s) will be rekeyed; if magnetic cards are lost or not returned, the code is changed and new magnetic cards must be issued; if a keypad entry, the keypad codes are changed if a staff who had authorization leaves that Company location or is terminated.

- Anytime a building is unoccupied by staff, the building's doors shall be locked. No consumers, visitors, or other unauthorized persons are allowed beyond the front entry area without being accompanied by a staff; they must be signed in at the door prior to accompanying any staff beyond the entry. The doors of rooms not in use are closed and, if appropriate, locked. Fire exit doors, if located in areas not directly visible to any staff, are kept locked but will have keypads, crash bars and/or manually operable deadbolts for exit in an emergency.

- No access to electronic media is to be available to unauthorized staff.

Workstations

- Computer based ePHI can be accessed from any workstation, with the appropriate log-in ID and password; workstation assignments are not required for use of computers.

- Department Managers/Supervisors and their staff have an assigned workstation for access to both ePHI and/or non- ePHI information within their personal profile.

- All workstations are to be kept locked when not in use by a staff. If a workstation does not have the capability of being locked, all electronics that store/access e PHI must be shut off when staff is not present and, if feasible, secured to avoid being carried off easily; if there are physical storage units containing PHI within a workstation, they must be kept locked anytime staff is not present.

Security When Away From Workstation

- When away from their workstation for an extended period, staff with access to confidential or sensitive information on their computers or other electronic media must do one of the following:

    - Lock the door to the area where the computer is located,

    - Log off their computer or other electronic media,

    - Turn off their computer or other electronic media, or

    - Enable screen saver password protection.

- All electronic media, whether Company owned or personally owned that store and/or accesses ePHI must have automatic log-off set at 5 minutes or less. This log off can be set up so that the screen goes blank or goes to a screensaver; either requires a password to re-enter.

Security during Maintenance, Repair, and Modification of Building Facilities and/or Equipment or Structures Containing PHI/ePHI

- QBH maintains its own maintenance and repair staff who handle most situations that require access to the buildings/facilities of QBH. Only occasionally are other sources required. When maintenance, repair or modification of electronic media is required, it is done by the contracted IT Consultant, based upon a task ticket issued by the CEO or Medical Records staff and authorized by the CEO; the IT Consultant goes to the location where the problem exists to do the activity required, unless the action can be accomplished remotely. A service receipt is completed by the IT Consultant; these tickets are available to the Security Officer via the CEO who retains the IT service receipts that reflect work done.

- Any time personnel are present to conduct maintenance, repairs or modifications to facilities where PHI/ePHI is present, a Department Director/Manager/Supervisor or other designated staff is present while the activities are occurring to monitor security of PHI/ePHI. If necessary, sources of PHI/ePHI storage and/or access may be removed, after being securely backed-up, unless web-based, from the area and locked in another workstation area until the activities are completed.

- A Maintenance Log is maintained by the Medical Records Coordinator and/or CEO, of all maintenance, repair, or modification to physical components of buildings/facilities which are related to security (hardware, walls, doors, locks, etc.) and/or of electronic or storage equipment containing PHI/ePHI. The log shall contain, minimally: what was required (maintenance, repair, or modification); to what; time and date begun and ended; what was done; who monitored ePHI/PHI; who did the maintenance, repair, or modification; and any security issues noted (if so, was Security Officer informed).

- The Security Officer shall maintain a log of the movements of hardware and electronic media, and any person responsible for these movements to include minimally: what is being moved, from where and to where it is being moved, time and date when the back-up was done prior to the move (if applicable), time and date of the move, who moved the equipment. If there has been no movement in a month time frame, the Security Officer will document on the log that there has been no movement during that month and the date of the entry.

Devise and Media Controls: Disposal or Re-Use of Electronic Media

- Anytime that Company-owned electronic media, including equipment with hard drives, memory cards, CDs or DVDs, flash drives, external drives, cell phones, etc., that contain ePHI/IIHI data are to be disposed of or moved to another location or user, they are to be *submitted to the IT Consultant so that all data can be removed before reuse or disposal.* The CEO will facilitate notification of and obtain a service receipt from the IT Consultant.

Staff's personal devises and media are not to store any PHI/ePHI data. Compliance will be verified by random inspections of staff's personal devises/media during routine surveillance activities by the Security Officer.

- Any data that needs to be transferred to a new devise will be transferred by the IT Consultant prior to removal of data. Likewise, if any electronic devise needs to be moved, the IT Consultant or Department Manager/Supervisor will do a secure data back-up of any non-web-based data, if not already backed up, creating an exact copy of any ePHI, prior to moving the equipment as a precaution against loss.

- See the Electronic Services Management Policy for further instruction regarding disposal and/or re-use of electronic media.

SECURITY: TECHNICAL SAFEGUARDS

PROTECTION

- PHI/IIHI should never be stored on the local "C" or shared "S" drives.

- Either the entire computer or other electronic devise, the files or folders containing ePHI/IIHI, or programs/software/applications containing ePHI/IIHI shall be encrypted, and password protected or stored in a secured cyber-network (such as Drobox or other cyber-networks).

    - The cyber-networks currently used by QBH use at least a 128-bit encryption and operates with an ID name and a secure password for system security.

    - Likewise, any disc, USB memory stick, external drive or other media that can store ePHI/IIHHI shall also be encrypted and password protected and/or Drobox or other cyber-network storage is used.

    - This applies to electronic media owned by QBH and personally owned but used to access, store or retrieve QBH related documents. QBH's IT Consultant will provide for this on QBH electronic media and provide instructions for how to encrypt other forms of personal electronic media as needed.

- Closed EMR data and individually saved ePHI is backed up via the network. If any QBH data is stored on Company-owned electronic media, that data should be backed up. The storage media used for back-up should be encrypted and password protected and stored in a secure location or Drobox should be used. *QBH's IT Consultant will provide directions for installation of encryption and password protection to offices/workstations and instructions for staff as needed.* Company PHI/ePHI shall not be stored on personal electronic media; nonetheless, staff is encouraged to use encryption and password protection on their personal electronic media as well as a general safety measure.

- Anti-virus, malware and firewall protection shall be in place on every QBH computer and on other electronic equipment if QBH information is stored, accessed or transmitted. *QBH IT*

Consultant will provide for this on Company electronic media and will provide instructions for how to install it on personal electronic media, if required. **ALERT: File sharing is one of the most common ways that computer systems become infected with malicious software.** The Network Server has its own malware and virus protection and the back up in web-based Dropbox has malware and virus protection maintained by the product Company.

- Any program/software/app to be downloaded or installed on Company electronic media is done by the IT Consultant, with the approval of QBH Accountant. The following guidelines are to be followed:

  - ✓ Only work-related programs/software/apps may be downloaded or installed on Company-owned electronic media.
  - ✓ No games, Facebook and/or related programs, or other types of programs/software/ apps not pertinent to job may be downloaded or installed on Company-owned electronic media, nor accessed or shared with consumers on personal electronic media/phones during work hours or while conducting Company business.
  - ✓ If the Department Director/Manager/Supervisor is unsure whether a particular program/software/app qualifies to be downloaded or installed, the Medical Records Coordinator should be queried to make a determination.

- Any program being downloaded or installed must be checked for virus or malware infection prior to being downloaded or installed; any with infections are resolved by the IT Consultant and the faulty product may be returned to the supplier. The IT consultant provides a service receipt to the CEO who provides a report of these services to the Security Officer upon request.

- Notification of the Security Officer (Medical Records Coordinator, if Security Officer is unavailable) should occur <u>immediately</u> by the Department Director/Manager/Supervisor or staff member if a virus or malware is detected. The Security Officer will promptly notify the CEO who will authorize intervention with the IT Consultant.

COMPUTER/ELECTRONIC MEDIA ACCESS, PASSWORD PROTECTION AND INTEGRITY

- All electronic media, individual profiles, and/or files/programs that contain ePHI must have a log-in requiring user ID and password protection. The CEO will oversee assignment of these for the network server and/or on Company electronic media. The job position dictates what profile code is appropriate; the CEO oversees selection of the log in and assigns a temporary password to each new user. The user provides answers to five security questions that can be used to verify that any request for a password change in addition to the server prompted 90-day changes, is coming from the appropriate user. The users then select their own password to replace the temporary password. The CEO has a list of the log-in unique user ID and password security question answers for each user. Only these persons are allowed access to this security information.

  - Each ePHI user's password is changed every 90 days; the network EMR system prompts for this change. A former password cannot be re-used. This requirement also applies to Drobox and other cyber-networks, if used.

- The CEO can reset a temporary password if a user forgets their personally selected password, which is never recorded by them or by anyone else. The user must correctly answer the security questions to be given a new temporary password.

- All staff is instructed to never share their password and to not write it down. Failure to comply may result in disciplinary action.

- A security matrix has been established that sets the profile codes for each job position and the rights applicable to each profile code. Only the CEO may test or modify this matrix.

- To qualify for access to any form of ePHI, the staff member must first have completed training for the system in use, access must be delineated in their job description, and a profile code must be established for their job position appropriate to their job requirements.

- Access to any Company-based program or program segments is assigned on a "need to access" basis which is referred to as a profile code as determined on the security matrix. Some access may be "read only" access, depending upon the position or nature of the need for access.

  - The network server system maintains strict security. Since the network server can only be entered by a person with an assigned id and password and because there is disciplinary consequence for password sharing, breaches are highly unlikely. If a staff sees evidence that someone other than themselves has accessed their profile, the Security Officer should be immediately notified. The Security Officer will investigate to confirm a breach and complete a report of the investigation and breach findings for prompt submission to the CEO. See the Breach Policy for further action to be taken.

    - ✓ The assigned profile code limits what the user may access and what they may do within the network server and Drobox or other cyber-network systems. These systems have been tested and cannot be breached.

    - ✓ In an emergency, the CEO can gain temporary access to an otherwise unauthorized area, referred to as "breaking the glass." Any attempt to "break the glass" by anyone else should be reported to the Security Officer immediately so that the Officer can immediately initiate an investigation. The Security Officer can initiate an audit trail to explore what was accessed, if anything, and whether anything was modified. In the instance where ePHI was exposed, the consumer is immediately notified of the breach and encouraged to stay alert and report anything that might help. The staff member is required to immediately change their password.
    - ✓ Personal electronic media, including phones, used by staff to access ePHI must be able to be locked and must be password protected.

- **It is imperative that passwords are sufficiently complex.** Do not use any of the following in selection of a password:

- Your birthday
- Your spouse's name
- Your child's or pet's name
- Your favorite sports team
- A password you commonly use

- Passwords for a network server profile or cyber-network access of a staff must contain a capital letter, a number, a symbol, and be at least 8 characters long.
- Do consider use of the following when selecting a password:
  - Intersperse characters into your password; the more characters used the more complex and resistant it will be to hacking.
  - Mixed characters are better than repetition of the same one. Use different characters mixed together with upper- and lower-case letters, numbers and symbols.
  - Do not use real words that can be found in the dictionary, in any language. If using words, add extra letters or omit letters and intermix with numbers, symbols, or characters.
  - Phrases can help memory. Use letters based upon a phrase familiar to you and mix with characters, numbers, capital letters, or symbols.
- If you think your password has been compromised, change it and report it to your Department Manager/Supervisor and the Security Officer immediately. If the password is on electronic media that is assigned by the CEO, notify the CEO immediately so that a new password can *be assigned.*
- Passwords are to be changed at least every 90 days. The staff member will be notified by the network when it is time to change their password. If the password is on personal equipment that transmits and/or receives ePHI, the password should be changed every 90 days and the Department Manager/ Supervisor informed so that the date of the change can be logged.
- Do not use the same password for all systems that you access. Also **do not write down your passwords** anywhere. If need be, you may write down a hint that will mean nothing to anyone but you and that will prompt you to recall your password. **Do not share your passwords unless it is essential, such as for a system repair and then change the password immediately after the repair.** Remember to follow the process described above with regard to a password change.

- Any time a request for change of password occurs, the user must provide correct answers to one or more of a set of security questions as prompted by the CEO. Only the CEO shall have access to the answers to each user's five security questions which are provided upon initial assignment as a user.

- See additional information related to electronic access later in this policy.

SUPERVISION OF EPHI USERS

- Clinical users are supervised by their Clinical Director. Non-clinical staff is supervised by their Department Manager/Supervisor.

    - If issues arise or concern exists by the staff or their supervisor, they may query the CEO.

TERMINATION FROM COMPUTER/ELECTRONIC MEDIA ACCESS

- Any staff member who is no longer qualified or eligible for the profile code assigned, for whatever reason, will be promptly unassigned within the applicable electronic system, by the CEO.

- When changes in profile code are needed due to job description/duties changing, a person's job position changing, or changes in needed information for QM purposes by the Quality and Infection Control Coordinators, the CEO can authorize those changes and change the profile code for that staff.

OTHER MECHANISMS FOR INTEGRITY

- The following types of information can be accessed and/or entered by only the persons noted below:

    - Read only access is specified by the profile code of some staff.

    - Data may be entered only by those with such authority based upon their profile code.

    - Forms and policies can be built by the CEO.

    - Billing reports can be generated and/or accessed by the Biller.

    - Billing input and changes can be done by the Biller.

    - Changes to forms and policies can be done by the CEO.

- Data that is transmitted or exported must be password protected and submitted in a pdf "read only" format so that it cannot be modified. Password information is transmitted in a separate document or email. Transmittals must be approved by the CEO.

- The network server has built in service locks once data is entered; it can be unlocked only by the CEO.

NETWORK SERVERS/ NETWORK EMR ELECTRONIC RECORD

- Network servers can only be accessed by entering authorized user ID names and passwords. These networks will be encrypted as well as password protected.

- Network security software will be utilized so that access to confidential or sensitive information is limited to staff that is entrusted by QBH to have access to such information.

    - Upon hire, applicable staff will establish a user ID and password.

    - The user ID will consist of the new staff member's first initial and last name. The password will be of the new staff member's choosing, following guidelines listed above.

    - Upon selection of a password, the new staff will be authenticated by the CEO and given appropriate network or designated computer and/or program access based on the username and password.

    - The CEO will maintain the list of computer, program, and network password security question answers in a secure fashion.

    - Rights to confidential or sensitive files will be assigned to profiles according to the type of access they need (i.e., read, write, modify, copy, delete, etc.). The CEO will apply the least restrictive rights that will maintain confidentiality and security.

    - In all departments or offices, passwords will be changed at least every 90 days and/or more frequently if determined necessary by the Medical Records Coordinator or CEO.

    - The CEO will maintain and update the user database regularly so that former staff members no longer have access to the network, and new staff members have appropriate access.

NON-NETWORK ELECTRONIC EPHI/IIHI INFORMATION

- All computers will be required to be encrypted and password protected. A daily back-up of any ePHI that is not web-based, following requirements for back-up media addressed earlier, will be done by the CEO.

- Mobile electronics with ePHI/IIHI that are easily removed or carried off shall <u>not</u> be left unattended and/or will be locked up when not in use.

- Media or containers containing ePHI and paper PHI are never left at an unauthorized location. If left at a worksite other than the office/department, it is kept locked in a cabinet or drawer within a locked room whenever unattended by responsible staff. During transport it is secured and locked within the vehicle or trunk of the vehicle.

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONFIDENTIALITY, SECURTY AND INTEGRITY OF INFORMATION**

EMAIL

- PHI/IIHHI is NEVER to be included in, stored in or attached to an email with the exception of those who have access to and send emails via the encrypted and password protected Company Intranet system. Emails on QBH Intranet system shall have a confidentiality statement similar to what is included on facsimiles. Emails from QBH Intranet system shall only refer to the first name of the consumer.

- The following is <u>never</u> to be included in an email other than encrypted and password protected Company Intranet emails:

    - Identifiable health information or identifiers or the consumer

    - Identifiable health information or identifiers or the family, relatives, employers or household members of the consumer

- Re-read any email before you send it to make sure the content is appropriate for the intended recipient(s). Consider who else might see the message.

- Always double-check that the "to" address is correct. Be especially careful when sending a "reply to all" or add "cc"/"bcc" addresses.

INSTANT MESSAGING, BLOGS, FACEBOOK AND OTHER SOCIAL NETWORKING MEDIA

- Instant messaging, blogging and Facebook or comparable media are not allowed for Company communications that include ePHI/IIHI of consumers, their families or Company staff.

- Staff shall not engage in blogging or Facebook (et al) communications with current or past consumers or staffs.

- Those with access to QBH Intranet may instant message within that system only and then any information should be the minimum necessary.

LOCATION

- All forms of electronic media shall be kept in physically secure, non-public locations whenever possible. If use in a public area is necessary, the computer/electronic media must be positioned so that it is safe from visitor access or viewing.

- Portable equipment (e.g., PDAs, any hardware upon which data is moved between systems (USB flash/thumb drive, CD/DVD, etc.) presents a tremendous security risk. Those using these items MUST carefully adhere to these guidelines:

    - Whenever possible the portable devise should be kept secure in QBH's offices.

- All portable devises must be encrypted, and password protected.
- Avoid keeping very much ePHI/IIHI on portable devices; instead use security enabled communication links to on-site data bases.
- If a portable device containing ePHI/IIHI is lost or stolen, report it immediately to the IT Consultant and Security Officer.

NOTIFICATION OF PRIVACY PRACTICES

CONSUMER NOTIFICATION OF HIPAA RIGHTS

- Enhanced access to PHI/ePHI is provided by the HIPAA mega rule. Consumers/guardians now have the right to request and receive health records in electronic form when it is reasonable for them to do so.
- The principle of confidentiality and Notice of Privacy Practices will be explained to all consumers during the intake process. A copy of the Notice of Privacy Practices is provided to the consumer/guardian at intake; electronic copy may be provided if requested by the consumer.
- If a change in regulation results in a revision to this Notice, the revised Notice shall be provided either directly, or via US mail to the last known address, to any current consumers/guardians.
- In addition to the security practices already addressed in this policy, consumer confidentiality will be maintained through the following measures:
  - Information contained in the clinical record, a picture of the consumer, or other identifying information, may not be discussed, viewed, or in any way made available without the express written permission of the consumer or guardian except as prescribed by law or regulation.
  - When questioned regarding an individual consumer's status by an individual outside of QBH, staff will neither confirm nor deny the request.
  - Any requests for information regarding a consumer will be referred to the consumer's Counselor, the Clinical Director, or the Medical Records staff.
- Disclosures will only be made after receiving a completed Release of Information Form or the Authorization for Disclosure of Substance Abuse or HIV Information Form specifying the information to be released, the dates during which the release is valid, the persons or Company requesting the information and valid signatures of the consumer or guardian and a witness. Only requests on the approved form will be acceptable. Only the Medical

Records staff or designee may provide such disclosures.

- The following situations do not require a disclosure by law:
    - Exchanges for the purpose of treatment. This means two providers involved in a consumer's care can exchange information without an enacted Release of Information Form.
    - Exchanges for the purpose of payment. A provider can bill a payment source without an enacted Release of Information Form.
    - Health care operations. QBH or its designees can perform quality management and data analysis either itself or through a Business Associate.
    - The consumer's identity has been "de-identified" whereby consumer information is disguised to remove ANY identifying features that could track one back to that consumer.
    - Release for the "greater good." Circumstances when the provider is required by law to break the consumer's confidentiality in order to comply with required reporting of child and/or elder or dependent adult abuse, there is a danger of physical harm to another person(s) and there is duty to warn or protect that person(s), a court order compels breaking confidentiality and privilege is not granted, notice for assistance in the case of a suicidal consumer once it is determined they are at risk and in immediate danger.
    - Discussion among staff and/or government officials and auditors who have programmatic and fiscal responsibility for services to the consumer are not disclosures. Contracts and intergovernmental agreements allow for the sharing of information for the purpose of coordination and fiscal control, as well as quality control. The Secretary of the US Department of Health and Human Services also has access to carry out mandated audits and, as needed, investigations of reported breaches of PHI/ePHI/IIHI.
- A copy of the Release of Information Form or Authorization for Disclosure of Substance Abuse or HIV Information Form will be filed in the consumer's records.

USES AND DISCLOSURES

DATA COLLECTION FROM CONFIDENTIAL RECORDS

- Data collection will be used for the following reasons:
    - To organize and produce consumer services statistics for administrative purposes related to, but not exclusively:
        - ✓ Care processes or outcomes,
        - ✓ Consumer safety,
        - ✓ Infection control,

- ✓ Performance comparisons & trends,
- ✓ Management or operations,
- ✓ Results of improvement efforts,
- ✓ To develop a system of abstracting data to facilitate third party reimbursement procedures,
- ✓ To coordinate and track regular computerized billings for services.

- Any data collection on a consumer, whether by interview, observation, or review of documents, shall be conducted in a setting that provides maximum privacy and protects the information from unauthorized individuals.

RELEASE OF CONSUMER INFORMATION

- See the Release of PHI Policy for additional directives in the release of consumer information.

- Consumer information release, in whatever form, shall comply with HIPAA regulations. See the HIPAA related policies for the entire process. The Medical Records Coordinator keeps an electronic log that includes the consumer's name, the type of release, the day the record content was released and to whom. Only the CEO or Medical Records staff may release or disclose consumer information.

- If a consumer record has been subpoenaed, and a signed Release of Information or Authorization for Disclosure of Substance Abuse or HIV Information accompanies the subpoena, a copy of the subpoenaed information in the consumer record may be released, excluding psychotherapy notes.

- If the subpoena is presented to QBH with a Release of Information or Authorization for disclosure of Substance Abuse or HIV Information attached, the Medical Records staff will gather and copy the documents requested and, if time allows, will UPS the documents to the attorney or parole officer designated in the subpoena. A copy of the documents sent will be made and retained with the subpoena in Medical Records and within the official medical record. Electronic copies shall not be used to satisfy a subpoena. See the Receipt and Response to Subpoenas Policy for further instruction on subpoenas.

- To request information from other agencies about active consumers, a staff member must have the consumer complete a Release of Information Form or Authorization for Disclosure of Substance Abuse of HIV Information Form. The original release will be filed by the Medical Records staff into the consumer's medical record. Under no circumstance will a blank release be included in the consumer's permanent record.

- QBH may release a consumer's medical record WITHOUT the consumer's written consent to the following persons or as otherwise authorized by law (see PHI HIPAA related policies for guidelines):

    - Attending and consulting providers currently providing health care to the consumer for the purpose of diagnosis or treatment;

- Providers who have previously furnished health care to the consumer if the records relate to the prior treatment;
- Ambulance attendants for the purpose of providing care to a consumer they are transferring;
- Private agencies that accredit providers;
- Providers for the purpose of conducting utilization and peer review, or quality assessment activities;
- Persons or entities that provide billing, claims management, medical data processing, utilization review or other administrative services to the consumer's health care providers;
- Legal representatives of the provider for the purpose of securing legal advice;
- Personal representative or administrator of the estate of a deceased consumer (if a representative or administrator has not been appointed, then to the following persons, in the order of priority, unless the consumer, before his or her death, or a person in higher order of priority, objected to the release of the records to such person in writing; (1) spouse, unless separated; (2) acting trustee of an inter vivo trust created by the consumer for the benefit of the consumer during his or her lifetime; (3) adult child; (4) parent; (5) adult sibling; or (6) guardian or conservator at the time of the consumer's death);
- Consumer's health care decision maker at the time of the consumer's death;
- Personnel of the Industrial Commission, employers of consumers filing industrial injury claims, or the legal representatives of those employers.

- While a written consent is not required to release to the above entities, QBH may elect to obtain one.
- QBH MUST release a consumer's medical record WITHOUT THE CONSUMER'S CONSENT to government and other entities that have statutory authority to request and receive consumer records, such as the Board of Medical Examiners and the Osteopathic Board, when if requests consumer records as part of a physician the Michigan Medicaid/Medicare entities, when investigating potential program fraud or abuse, MI Department of Health Services (DHS) or the local health department when investigating communicable diseases, or a peace officer or protective services worker investigating child abuse, licensing and certifying entities as stipulated by state or federal law, the US Department of Health and Human Services during an audit or for the purposes of a reported breach investigation.
- Any requests for release of information with or without consent that are questionable will be reviewed by the Medical Records staff, the CEO and/or QBH's attorney as required.

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONFIDENTIALITY, SECURTY AND INTEGRITY OF INFORMATION**

SECURITY AND IDENTIFICATION OF VIP/HIGH PROFILE CONSUMER RECORDS

- QBH will maintain the confidentiality of high-profile consumers, including government representatives, i.e., mayor, governor, etc., physicians, relatives of staff, and all high-profile individuals with a public reputation.
    - Medical records of high-profile consumers will be kept in a confidential electronic record that is only accessible to the authorized caregiver; the Medical Records staff or CEO may also access these records.
    - The Medical Records staff will do loose filing in these records. If a consumer is related to the Medical Records staff or CEO, only the others of the two will access that record. A consumer is never assigned to a caregiver to whom they are related or have a personal relationship outside QBH.
    - On direction from the CEO, Medical Director, or a psychiatrist, any paper records will be placed in a secured (double locked) file. If electronic, special limited access will be arranged. Access to any paper secured file is documented on the log sheet located in the front of each drawer in the secured cabinets.
    - Media calls regarding any high profile/VIP consumer will be directed to the CEO.
    - Requests for release of information regarding high profile/VIP consumers will be directed to the CEO.

STAFF CONFIDENTIALITY

- Staff information will be maintained confidential through the following measures:
    - Staff will neither confirm nor deny requests regarding an individual's employment or contract status. Requests for information regarding a staff member will be referred to the Human Resources Manager.
    - Access to personnel records will be limited to the following on an "as needed" basis:
        - ✓ The Human Resources Manager and CEO will have access to all personnel files.
        - ✓ **Supervisory staff will have access to the files of staff that they** supervise.
        - ✓ Individual staff members will have access to their own file under supervision of the HR Manager.
        - ✓ Legal, regulatory, accrediting, and consultants, as applicable to their roles with QBH may access personnel files during the conduct of their monitoring activities.
- Information contained in the staff member's personnel record may not be discussed, viewed, or in any way made available without the express written permission of the staff, except as prescribed by law or regulation, with the following exceptions:

- Information necessary to keep a staff member and/or their supervisor informed on performance and/or training requirements or deficiencies may be transmitted electronically only under password protection.

- Any other information within staff's personnel files requires a specific Release of Information before the information may be released. This release shall be retained in the person's personnel record.

- Any visitor to QBH requesting to see a staff member will check in and be provided a QBH visitor badge.

  - The receiving staff will then notify the staff of the visitor's name.
  - The staff will inform the receiving staff if he/she wishes to see the visitor.
  - If so, the staff will meet the visitor in the entryway and then, if necessary, escort the visitor to the appropriate location in the facility.

CONFIDENTIALITY AND BUSINESS ACCESS

- In order to conduct the business of QBH, there will be persons that will need to visit our locations to carry out the business of QBH. These persons might include, but not exclusively, UPS/FedEx Delivery persons, housekeeping service staff, maintenance/repair persons, Fire Department representatives, etc. These persons will need to sign a Business Access Confidentiality Agreement when they enter QBH's sites. If a person is a repeated visitor to QBH's sites, they need only sign the form one time.

- The Human Resources Manager shall maintain a file of the original completed Forms; the Department Director/Manager/Supervisor may retain a file with copies of these completed Forms. The Privacy Officer shall periodically review this file for compliance and collect the contents of the file annually to retain as evidence of compliance during an audit.

LOGS/REPORTS REQUIREMENTS

- In addition to reports already addressed in this policy, QBH shall maintain ongoing logs or reports, mostly using BI Reports when possible, to include at least the following:

  - Audits by authorized persons conducted of electronic and paper PHI shall be maintained by the Medical Records staff or designee.

  - Access reports of all actual and attempted access to PHI and/or ePHI shall be maintained. The CEO and the Medical Records Coordinator can access these from the Network Server. Any breach of non-Network PHI/ePHI shall be documented in appropriate Privacy and/or Security Officer Investigation Reports.

- Logs, maintained by the Medical Records staff or designee, shall be maintained of all releases of PHI in whatever format to include the date and time, to whom it was released, what was included, whether the consumer release was obtained, if required, and who released the information.

- Security incident tracking reports of any unauthorized disclosure, use, access, loss or theft of PHI or equipment containing PHI, and any other security breach related to PHI shall be maintained by the appropriate Privacy or Security Officer.

- Maintenance/repair logs, in the form of a Service Receipt, are maintained by the CEO.

- Password Change Logs are maintained for a period of six years.

    - If any password changes are required besides the one prompted by the EMR system every 90 days, for whatever reason, the password change must be logged by the CEO who will maintain the log.

    - Non-Network ePHI password changes on Company-owned electronic media and/or programs/folders within a Company-owned electronic media source are to be done every 90 days. The 90-day change and any changes occurring in the 90 day interim are to be logged on the Password Change Log by the CEO.

    - No staff is to maintain ePHI on their personally owned electronic media. Compliance is monitored by random checks of personal electronic media by the Security Officer; if any is found and must be wiped, it will be wiped by the Security Officer or by the owner and verified by the Security Officer; the finding and action will be documented in the Security Officer's inspection report. A Disciplinary Action Form will be initiated on the staff member by the Security Officer and submitted to HR for placement in the staff's personnel file. A second violation shall result in disciplinary action as determined by the Clinical Committee.

- A Media Movements Log is maintained by the CEO that lists movements of Company-owned hardware and electronic media and any change of persons responsible for them.

- These logs and reports shall be made available to the Security Officer upon request, to auditors from regulatory, accreditation, state inspection personnel, and to the US Department of HHS in the case of an audit or investigation.

- These logs and reports shall be retained for a period of six years and shall be maintained in a secure, tamperproof manner whether in paper or electronic format.

DATA VALIDITY

- Each user develops documentation on the internal procedures of each work station including but not limited to:

    - Gathering of information for data entry.

    - Samples of source documents used for input.

    - Schedule of required reports.

- Reports to keep, and how long.
- Logging on to terminals.
- Logging off.
- Leaving adequate audit trail.
- Performing or requesting routine maintenance.

HANDLING EXCEPTIONS

- Users do not modify menus, screens, templates, data file structure, or report forms prepared for their use by second parties without approval from the author and/or their supervisor. Contacts with vendors outside QBH involve the CEO, including consulting before placing the initial call related to a problem, and reporting the outcomes.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

- For some staff to accomplish their job duties, de-identification of PHI/ePHI/IIHI may be necessary. QBH determines that health information is not individually identifiable health information if the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed.
  - Names;
  - Addresses;
  - Telephone and fax numbers;
  - Electronic email addresses;
  - Social security numbers;
  - Medical record numbers;
  - Health plan beneficiary numbers;
  - Account numbers;
  - Certificate/license numbers;
  - Vehicle identifiers and serial numbers, including license plate numbers;
  - Internet Protocol (IP) address numbers;
  - Biometric identifiers, including finger and voice prints;

- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

- Text messaging, by any method, of consumer, staff or business information is prohibited, except for staff with access to the encrypted and password protected Company Intranet. In no circumstances should information above be included via these media. Staff that receives such transmissions is required to report it promptly to the Security Officer. Non-compliance with this policy may result in disciplinary action and/or termination.

- QBH may determine that health information is not individually identifiable health information if QBH does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

- QBH may assign a code or other means of personal identification to allow information de-identified under this section to be re-identified by select QBH staff in the course of their job duties, provided that:
  - The code or other means of consumer/staff or consumer/staff record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
  - QBH staff authorized to use coding does not use or disclose the code or other means of identification for any purpose and does not disclose the mechanism for re-identification. The code re-identification data is kept secured in an encrypted and password protected manner at all times; no paper copy shall exist.

MINIMUM NECESSARY REQUIREMENTS (PROFILE CODES)

- QBH must identify:
  - Those persons or classes of persons, as appropriate, in its workforce that need access to protected health information to carry out their duties; and
  - For each such person or class of persons, the category, or categories, of protected health information to which access is needed and any conditions appropriate to such access.
  - QBH must make reasonable efforts to limit the access of such persons or classes identified to PHI consistent with the protected health information that they need to carry out their duties.

- For any type of disclosure QBH makes on a routine and recurring basis, QBH shall implement protocols/criteria that limit the protected health information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

- For all other disclosures, QBH must disclose information reasonably necessary to accomplish the purpose for which disclosure is sought; and Review requests for disclosure on an individual basis in accordance with such criteria; and QBH has a disclosure complaint process within the HIPAA policies related to disclosure of PHI/ePHI/IIHI as required by law.

- QBH may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

  - Making disclosures to public officials that are permitted in compliance with QBH HIPAA policies on disclosure, if the public official represents that the information requested is the minimum necessary for the stated purpose(s). Such disclosure may only be provided by the CEO;

  - The information is requested by another Company that is HIPAA compliant; or

  - The information is requested by a professional who is a member of its workforce or is a Business Associate of QBH for the purpose of providing professional services to QBH, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).

- QBH may not use, disclose or request an entire clinical record, except when the entire clinical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

LIMITED DATA SET

- A limited data set is PHI/ePHI/IIHI that excludes the direct identifiers of the individual or of relatives, employers or household members of the individual as listed earlier in this policy.

- No limited data set may be disclosed without authorization from the consumer or guardian.

- QBH may disclose a limited data set to a Business Associate only for the purposes of research, public health, or health care operations.

- QBH may disclose a limited data set only if QBH obtains satisfactory assurance, in the form of a data use agreement, that the limited data set recipient will only use or disclose the PHI/ePHI, IIHI for limited purposes.

- A data use agreement between QBH and the limited data set recipient must:

  - Establish the permitted uses and disclosures of such information by the limited data set recipient.

  - The data set agreement may not authorize the limited data set recipient to further use or further disclose the information in a manner that would violate the requirements of HIPAA;

- Establish who is permitted to use or receive the limited data set; and
- Provide that the limited data set recipient will:
  - ✓ Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;
  - ✓ Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;
  - ✓ Report to QBH any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;
  - ✓ Oversee that any agents, including a subcontractor, to whom it provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient; and
  - ✓ Not identify the information or contact the individuals.
  - ✓ If QBH becomes aware of a pattern of activity or practices of the limited data set recipient that constitute a material breach or violation of the data use agreement, QBH will implement reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful, QBH will:
    - ➢ Discontinue disclosure of protected health information to the recipient; and
    - ➢ Report the problem to the Secretary of the U.S. Department of Health and Human Services or designee.

CODE SETS

- QBH is required to apply for and obtain a National Provider Identification (NPI) from the National Provider System for itself and any subpart entity that would be a covered health care provider.
- Likewise, QBH is required to acquire a unique employer identifier (EIN).
- QBH is required to use the official DSM 4 or 5 Guidelines and/or CPT codes for coding and reporting of medical data.
- Medical Record Management and other HIPAA related policies define additional procedures and/or these procedures in more detail.

EVALUATION

- This policy will be reviewed and as needed, revised, annually (every 12 months +/- 30 days) by the Security and Privacy Officers and, as needed, the IT Consultant. With reports submitted to the Clinical Committee on needed revisions for approval.
- Evaluation shall also include at least annually:

- A Risk Analysis, facilitated by the Privacy and Security Officers, to identify potential risks/vulnerabilities to confidentiality, integrity and availability of PHI/ePHI/IIHI.

- Applications and Data Criticality Analysis to assess relative criticality of specific applications and data to support contingency plan components.

- Quarterly reports by the Privacy Officer and Security Officer, for ongoing monitoring of HIPAA/HITECH compliance and any specific issues or trends needing leadership action.

FORMS

Personnel Confidentiality Affidavit
Release of Information Form
Authorization for Disclosure of Substance Abuse or HIV Information
Risk Analysis Form
Maintenance/Repair Log
Password Change Log
Record of Movements Log

CONFIDENTIALITY

MEDICAL RECORD AND SENSITIVE INFORMATION CONFIDENTIALITY PRACTICES

- All medical records are the property of QBH and will be maintained to serve consumers and health providers.
- The consumer has the right to have the information in his/her record protected. All consumer information is regarded as confidential and made available only in accordance with HIPAA guidelines.
    - Consumers may access their own information upon written request unless, after review by the Clinical Director, documentation of a clinical reason why the consumer should not have access is provided and included in the consumer's medical record. In this case the consumer will be informed that the denial of review may be appealed to the Recipient Rights Advocate.
        - Review of the record by the consumer shall be under the Clinical Director or designee's surveillance.
        - If a consumer requests a copy of their record, it shall be delivered to them, but they will be required to pay the costs of photocopying.
- Staff members having access to medical records and other sensitive information are required to abide by the confidentiality standards of this policy. Staff sign an affidavit of their intent to abide by these standards at the start of their employment or contract.
    - Confidential and sensitive information at the Reception Area must be always covered or blocked from view of unauthorized persons.
    - Rooms containing any consumer or Company confidential records must be locked when not occupied by an authorized staff.
    - File cabinets containing confidential or sensitive information will be locked when vulnerable to unauthorized persons.
    - Keys to medical record rooms, staff offices and other locked areas will be assigned only to authorized staff; authorized staff is responsible for protecting the areas to which they have been assigned keys and to always keep the keys in their possession.
    - Incoming faxes are retrieved by a designated staff and distributed directly to the intended recipient.
    - Incoming mail will be date stamped and promptly forwarded to the intended recipient. Outgoing mail will be placed in a bin in the office of the staff member responsible for mailings.
    - When staff is away from their workstation, staff will lock their office, log off of or turn off their computer, or enable screen saver password protection.
- Confidentiality is explained to consumers during the intake process.
- Information contained in the medical record, a picture of the consumer, or other identifying information may not be discussed, viewed, texted, emailed or in any way made available without the express written permission of the consumer or their legal guardian/representative except as prescribed by law or regulation.
    - When questioned about a current or past consumer by an individual outside QBH, staff shall neither confirm nor deny the request for information or the consumer's status with QBH.
    - Any legitimate requests for information (such as from a provider or guardian) will be referred to the consumer's case manager, counselor, or the Clinical Director.
    - Disclosures will occur ONLY after receipt of a completed and signed Release of Information Form by the consumer (see requirements below).

- Any request for medical record information with or without a consent that is questionable will be reviewed by the Medical Records staff, the CEO and QBH's attorney as required.

RELEASE OF CONSUMER MEDICAL RECORD/INFORMATION

- Unless specifically authorized by state or federal law or regulation, by HIPAA compliance guidelines, or the consumer's specific written authorization for release of all or part of their medical record, all consumers' medical records are maintained as confidential.
  - Medical record information may be shared internally within QBH among clinical staff involved in the consumer's care.
  - Medical record information may be accessed for quality, utilization and record maintenance purposes by staff so authorized in those functions.
  - Medical records may be released to outside parties who are legally authorized or required to have access to that information such as the court when treatment is mandatory, a fiscal entity for payment or entitlement determination, or through subpoena.
  - Medical record information may be reviewed by regulatory and/or accreditation bodies as part of licensing, accreditation, or grievance activities.
  - Medical record information may be released to whomever the consumer has authorized through a written *Release of Information* process compliant with HIPAA regulations.
  - Medical record information related to chemical dependency, including lab test results, may never be released without the specific written consent on an *Authorization for Disclosure of Substance Abuse or HIV Information* of the consumer or their guardian/representative.
- *Release of Information* forms are maintained and utilized in compliance with HIPAA regulations and any other applicable state or federal laws. The *Release of Information* or *Authorization for Disclosure of Substance Abuse or HIV Information* form is a part of the medical record once completed and signed by the consumer and/or guardian.
  - The Release of Information form must have the following items completed for it to be legally employed for the release of medical information:
    - The name of the person about whom information is to be released.
    - The content to be released.
    - To whom the information is to be released.
    - The purpose for which the information is to be released.
    - The date on which the release is signed by the consumer and/or guardian.
    - The date, event, or condition upon which the authorization expires.
    - Information as to how and when the authorization can be revoked.
    - The signature of the consumer, guardian or legal representative authorized to sign the release. This signature shall be witnessed, and the witness shall also sign and date that they witnessed the signature.
- The photocopying/preparation and release of consumer information to a party external to QBH is done by the Counselor and documented in the consumer's medical record, including notation of what information was provided, to whom it was provided, the date and time it was released and in what manner it was released (certified mail, confidential facsimile, courier, face-to-face exchange, etc.), and the date of the signed Release of Information that authorized the release, if applicable.

SUBPOENAS

- If all or a portion of a medical record is subpoenaed and a signed *Release of Information* accompanies the subpoena, a copy of the subpoenaed information in the medical record may be released.
- If the subpoena does not include a signed *Release of Information*, the Medical Records staff will forward the subpoena, or direct its delivery, to the CEO or Clinical Director who will file an objection to the subpoena and the paperwork will be forwarded to the Medical Records staff to be filed in the consumer's medical record.

GOVERNMENT/STATUTORY AUTHORITY AGENCIES

- QBH will release a consumer's medical record WITHOUT THE CONSUMER'S CONSENT to government and other entities that have statutory authority to request and receive medical records.

INDIVIDUAL MEDICAL RECORD MANAGEMENT GUIDELINES

MEDICAL RECORD CONTENT
(NOTE: medical record, consumer record, and clinical record are used interchangeably among MAT policies.)

- The medical record is electronic, except for the consumer orientation, consent and authorization forms, Assessment: Part I and Integrated Assessment: Part I, all nursing documents, and any documents that come from outside sources, all of which are in hard copy. These hard copy documents are not currently scanned and added to the electronic record.
- A copy of the electronic documents and all hard copy documents are maintained as a full hard copy in the Medical Records Room; this is considered the official primary medical record as it contains all record elements. The electronic record is considered a secondary record at this time.
- If more than one family member is being treated in the MAT program, each shall have their own separate medical record.
- The medical record must contain the following data to be considered a legally satisfactory record:
  - The name, address, date of birth, and sex of the individual served.
  - The date of admission.
  - Preferred language and any special communication need(s) of the consumer.
  - Information about the consumer's guardian, legal representative, or representative payee, if applicable, including that representative's name, address, and phone number.
  - Information about a person to contact in event of an emergency, including their name, address, and phone number.
  - The name of the person currently coordinating services of the consumer served.
  - The location of any other records.
    - The electronic record will reference any hard copy documents that are not part of the electronic record.
  - Information about the consumer's primary care physician (PCP), including their name, address, and phone number, if known by the consumer and, if applicable.
  - Healthcare reimbursement information, when applicable; or other financial agreement.
  - Consumer information including:
    - Reason(s) for admission or initiation of care, treatment, or services
    - Any emergency care, treatment, or services provided prior to arrival for treatment, if applicable

- Initial diagnosis, condition(s), or circumstances requiring care initially and during the curse of treatment
- Any allergies to food or medication
- Health history (including conclusions drawn from a medical history and physical, if applicable)
- Current medications and any ordered or prescribed
- Documentation of orientation
- All applicable assessments and reassessments, including findings
- Relevant observations and responses to care, treatment, or services
- Progress notes
- All medications administered, including strength, dose, route, date and time of administration, access site, administration devices used and rate of administration (if applicable)
- Any adverse drug reactions and interventions
- Any orders for diagnostic and therapeutic test and procedures and the results
- Master Needs List, treatment goals, and Personalized Treatment Plan (PTP), including reviews (Status Reports)
- Transition Plan
- Discharge Summary which is concise and contains the reason(s) for acceptance to treatment, the treatment provided, the consumer's condition at discharge, written discharge instructions/medications taken by the consumer at discharge/follow-up care instructions that was provided to the consumer, and family, if applicable.
  - ✓ If time in treatment was brief a final progress note may substitute for a discharge summary.
  - ✓ If the consumer is transferred to a different QBH program with different staff, a transfer summary can substitute for a discharge summary. If staff is the same in both programs, a progress note may be used.

- Correspondence pertinent to the consumer
  - Authorizations for release of information
  - Documentation of internal and external referrals or consultations.
- As needed or applicable to provide care, treatment, or services, the clinical record contains the following additional information:
  - Any advance directive
  - Any informed consent
  - Any documentation of protective services
  - Any documentation of consent by the individual served, family, or guardian for admission; care, treatment, or services; evaluation; continuing care; or research
  - Any records of communication with the individual served, such as telephone calls or e-mail
  - Any documentation of involvement in care, treatment, or services by the individual served and, when necessary, their family
  - Any information on unusual occurrences, such as complications; accidents or injuries to the individual served; procedures that place the individual served at risk or cause pain; other illnesses or conditions that affect care, treatment, or services; or the death of the individual served
  - Any indications for and episodes of special procedures.

MEDICAL RECORD ORGANIZATION

- The medical record has a standard order for content that is to be maintained by all staff having access to the record and is overseen by the Medical Records staff that is responsible for the filing of all medical record documents. That order is as follows:
  - Confidential Cover Page
  - Consumer Orientation
  - Consents/Authorizations/Releases of Information/Rights Statement
  - Assessments
  - Master Needs List
  - Treatment Plan/Treatment Plan Reviews/Treatment Plan Amendments
  - Progress Notes documenting each significant contact with the consumer and all treatment provided, reports of process and factors considered in decisions impacting treatment or changing treatment
  - Group Notes
  - Didactic Response Sheets
  - Daily Consumer Activity Report (DCAR)
  - Documentation of compliance with the MI approved central registry system to avoid dual registration by the consumer
  - Nursing Section
    - Assessment: Part 2
    - Vital Signs
    - Medication Log
    - Nursing Notes
  - Medical Section – if applicable to the program
    - History and Medical Exam
    - Prescription Copies
    - Doctor Orders/Standing Orders
    - Psychiatric Evaluation
    - Medication Reviews
    - Medication Consent Forms
  - Lab Results
  - Case Management
  - Reports of results of case conferences for the consumer
  - Record of correspondence with consumer, family, others, referrals, and results
  - Medications
  - Transition/Discharge Summary and Transition/Aftercare Plan
  - Miscellaneous
- Completed *Release of Information* Forms are retained in a secured drawer or cabinet within each counselor's office for their consumers for quick reference until the consumer is discharged at which time they are filed in the closed medical record of the consumer.
- The record is contained within a three-ring binder. Each record has a label identifying it, which includes: the consumer's last name followed by their first name, the consumer's date of birth, the consumer's insurance, the last four digits of the consumer's social security number, the program the consumer initially entered and the admission date. There is an insert on the front cover of each medical record that states: QBH, INC., Confidential Medical Record.
- Forms authorized for use in the medical record must be approved by the Clinical Committee for use or modification/revision. Staff responsible to use any approved form will be trained by the Clinical Director or designee prior to their initial use of the form.

- Incident reports are NEVER part of the medical record; they are securely stored in the office of the Utilization and Quality Manager.

TIME FRAMES FOR MEDICAL RECORD ENTRIES

- Consumer Orientation:
  - Outpatient MAT – during intake
- Assessments:
  - Assessment Part I – is completed at intake
  - Integrated Assessment: Part I – is also completed at intake
  - Integrated Assessment: Part II – during intake
  - Integrated Assessment: Part III – part of the intake
  - Physical Examination – within 14 days of intake
  - Psychiatric Evaluation is done within 72 hours after ordered, if indicated needed
  - Documentation of good faith effort to verify the consumer is not enrolled in any other MAT program
  - Other assessments are done as ordered by the Medical Director and/or Counselor
- Integrated Summary is due by the second appointment
- Treatment Plan:
  - Interim – during intake
  - Initial –by first counseling session
  - Updates – every 90 days for first year of continuous treatment, then semi-annually in subsequent years, including an evaluation of existing treatment plan and consumer's response
- Progress Notes – ongoing by end of shift when treatment/session/group was conducted
- Transition/Aftercare Plan – commences by first counseling session
- Discharge Summary –24 hours after discharge

CONDITIONS FOR MEDICAL RECORD DOCUMENTS

- All entries to medical record documents are to be legible, written in black ink, easily read, dated and either manually or electronically signed by the original writer.
  - Illegible and/or unreadable documents will be returned to the author to be re-written, if necessary, by the Medical Records staff.
  - If a document completed by a consumer is illegible and/or unreadable, the staff assisting the consumer in completion of the document shall review the content with the consumer and draft an identical legible/readable copy or may offer to write the information into the form for the consumer as they would if the consumer cannot read or write.
  - Any documents completed in the consumer's language will be re-written into English by a staff or a translator under the staff's supervision.
  - Signature stamps shall not be utilized at the QBH MAT program.
- Any document prepared for the medical record must be completed and submitted for filing by the end of the shift in which the interaction with the consumer or a collateral source occurred.
  - The document must be fully completed, signed, and dated before submitted for filing; if an area or section of a form is not applicable for a particular consumer, N/A should be written in that area or section.
  - Any unused spaces of a narrative section should be lined out.

  - Any incomplete document will be returned to the author for completion prior to filing by Medical Records staff.
- If a correction must be made, the erroneous content should be lined through with a single line, dated and initialed by the author. WHITE OUT or obliteration is never acceptable.
- Post-it notes, paper-clipped notes, etc. are not to be left in a medical record. If it is content that should be in the record, it should be taped to a progress note page and entered in the appropriate record section. Blank, unused forms are not to be kept in the medical record.
- Time frames for entry of various documents are set forth above and in policies related to those documents; submission is required to be timely.
- Only approved abbreviations and symbols (see list) may be used in the medical record and/or on any forms; likewise, abbreviations from the Do Not Use list (see list) may never be used in the medical record and/or on any forms.
  - Staff may request additions at any time by submitting their request to the Clinical Director who will bring those requests to the Clinical Committee for approval.
  - Once approved the Administrative Assistant/Office Manager will update the list, place the revised list in the Policies and Procedures Manual, and make the updated list available to all clinical services personnel.
  - These lists will be reviewed, minimally, with all new staff who will document in the medical record during orientation and to all staff that document in the medical record on an annual basis.

MEDICAL AND VERBAL ORDERS

- Verbal orders may be provided only to a nurse of QBH by physicians and/or other Company privileged independent providers of medical services.
  - The receiving nurse will write the verbal order into the medical record of the consumer.
  - The receiving nurse will read back the order to the medical practitioner providing the order and request verification of the accuracy of the order s/he has written.
  - The receiving nurse will sign and date the order and denote NRBV (*n*ote *r*ead *b*ack to medical practitioner providing the order for *v*erification of accuracy) after the order.
- The LIP shall review, sign and date the verbal order within 72 hours. Nursing will tab the order for the physician or other medical practitioner who gave the verbal order to sign.
- Written medical orders may be written only by a Company privileged physician or another Company privileged medical practitioner.
  - Medical orders must be clear, legible, dated and signed by the practitioner, including the practitioner's credentials.
  - Pre-printed orders may be used ONLY if they have been modified to fit the specific consumer, is signed by the practitioner before or within 24 hours of being implemented for the consumer, and the pre-printed order has been reviewed and approved by the Medical Director and Clinical Committee within the past twelve months as so noted in a footnote added to the pre-printed order and documented in Committee minutes.
    - ✓ Standing orders for admitting a consumer to the MAT program are not acceptable.
  - Orders written for medication and/or lab and other diagnostic tests must include the reason for the order and/or the diagnosis to which it applies.

MEDICAL RECORD STORAGE

SECURE STORAGE AND ACCESS

- Any records removed from the Medical Records storage area are to be signed out and returned by the end of the staff member's shift; only designated staff may remove records from the storage area. The record will be maintained in a secure and confidential fashion while in the staff's possession.
  - Medical records are never to be removed from the facility.
  - Medical records are never to be left unattended or where they can be viewed by those without authority to have access to the record.
  - There is to be no copying or duplication of medical record content without CEO approval.
- To provide safety, security and to maintain confidentiality, the Medical Records storage area is kept locked when not being attended by Medical Records staff. Records are secured in locked file cabinets as well. Only counselors and nurses have keys to access the active Medical Records storage area. The CEO is to be notified immediately if there are any breaches to this security process.

CLOSED MEDICAL RECORDS

- Hard copy closed records are maintained in the same order as the open record except they are filed in an envelope instead of a binder. Electronic records are stored in the computer network after closure.
- Each admission to treatment at QBH is maintained in a separate envelope after discharge; however, the envelopes are stored together.
- All closed medical records are stored in a separate locked medical records room within cabinets that are also locked.
  - The only persons with access to this storage room are the Medical Records staff, CEO and Recipient Rights Advisor.

RECORD RETENTION, RETRIEVAL AND DISPOSAL

- Closed hard copy medical records are stored and accessible for 7 years after which time they are disposed of through shredding by the Medical Records staff. Electronic closed records are retained perpetually.
- Any clinical staff, except monitors, is authorized to review these records but must retrieve them through one of the persons who have keys to that room.
  - Staff must sign the record out on a designated sign out sheet.
  - Records signed out must be returned by the end of the staff's shift. They are returned to a designated bin in the open medical records room and returned to the closed medical records room by Medical Records staff that documents the return on the sign out sheet.

EMERGENCY EVACUATION OF MEDICAL RECORDS

- Areas from which medical records might need to be evacuated include:
  - Nursing office
  - Medical records room

  - Closed records storage area
- First priority in an emergency evacuation is consumer and staff safety. If staff is not in immediate danger and an emergency requiring record evacuation exists, the Medical Records staff will oversee removal of records. If this staff is not available, the nurse in charge, or designee, will assume oversight.
- Any medical records that have been signed out will be the responsibility of the staff that has the records to evacuate, if possible.
- Nursing staff will be responsible for removal of medical records/record elements from their area.
- If removal is not possible, the Medical Records staff and nurse in charge will be responsible to see that their areas are secured with doors and windows closed and locked.
- Once all records that could be removed are gathered at the offsite location designated by the Emergency Plan, the Medical Records staff or designee shall organize and file the records in as secure a place as possible within the offsite location.
- Electronic records are saved to an offsite server and would be retrievable anywhere there is internet access.

EVALUATION

This policy shall be evaluated at least annually (every 12 months +/- 30 days) and as needed by the Security and Privacy Officers based upon findings from testing or actual implementation of the plan. It shall be submitted to the Clinical Committee for approval. Likewise, these Officers will report on testing and/or actual performance of the plan in quarterly reports as appropriate and at least annually in the form of an overall evaluation

FORMS:

ALL medical record forms (see Electronic Record and/or Medical Records Template Folder)
Release of Information Form
Closed Medical Record Sign-Out Form – available in Medical Records
Active Medical Record Sign-Out Form – available in Medical Records
Abbreviations and Symbols List
Do Not Use Abbreviations and Symbols List

QUALITY BEHAVIORAL HEALTH, INC. **MAT CONTINGENCY PLANNING-HIPAA/HITECH POLICY**

POLICY STATEMENT

- It is the policy of QBH to maintain plans for any contingency that may cause interference to QBH's information system and documents generated by that system. The system has three distinct but interrelating components:

  Data Back-Up Plan

  Disaster Recovery Plan

  Emergency Mode Operation Plan

Privacy and Security Officers are appointed to oversee the development, testing and, as needed, evaluation of implementation of the contingency plan. QBH is committed to provision of the resources necessary to the development, testing and, as needed, implementation of this plan. (See the Technology Plan and Information Management Policy for more information.)

DATA BACK-UP PLAN

- For each major application, at least 1 (one) backup person is trained to take over in the event of absence or transfer of the primary user.

- Measures are taken so that data recovery is possible in the event that records are lost, damaged or destroyed. For the Contingency Plan, Emergency Operations Mode Plan and Disaster Recovery Plan included with QBH's HIPAA/HITECH Policies.

- Computer network/program backups are performed daily for the EMR. Backup data is restored in the event that any computerized record is lost, damaged or destroyed. Any sensitive information not backed up in a cyber-network shall be backed up to mobile back-up media at a frequency set by the CEO, by the CEO or designee.

  - Mobile back-up media such as thumb drives, CDs/DVDs or external hard drives used on Company electronic media are to be scanned by the user for virus or malware infections before use. The same practice of checking is recommended for staff with their personal electronic media, especially if that media is used to access patient ePHI/IIHI.

DISASTER RECOVERY PLAN

EMERGENCY EVACUATION OF HARD COPY AND/OR ELECTRONIC PHI/EPHI/IIHI

- The areas from which such records might need to be evacuated are:

  - Record storage area and, potentially, clinical staff work areas

  - Records storage areas in Nursing Station/Nursing Office

  - Electronic media workstations

- The first responsibility is for patient and personnel safety. If personnel are not in immediate danger and an area fire breaks out, the following procedure is to be followed. The Medical Records staff, Clinical Director and Nursing Director will oversee the removal of confidential records/electronic media in their respective areas. If this person is not available, a pre-assigned designee will assume oversight.

- In the case of a fire:

    - All available staff (within a department) or Medical Records staff will be responsible for removing any current records, including medication records, located in their area or in filing cabinet(s) and any electronic media used to store ePHI/IIHI.

    - The Medical Records staff, Nursing Director and Clinical Director or designees will be responsible for coordinating the removal of confidential records/electronic media from their respective departments and workstations. If removal is not possible, they or their designees will see that file cabinets, doors and windows to these area(s) are closed and locked.

NON-FIRE DISASTER REQUIRING EVACUATION

- First responsibility is for patient and personnel safety. The clinical staff will be responsible for removal of records/electronic media/medication cart in their areas to the designated area as defined in the Emergency Preparedness Plan.

- The Medical Records staff, Nursing Director, Clinical Director or designee will be responsible for overseeing that confidential records are boxed and removed to designated areas as defined in accordance with the Emergency Preparedness Plan and that electronic media are safely removed.

- After all current hard copy records have been removed, all closed confidential records shall be boxed and removed if time allows.

- Hard copy confidential records still in the area will be boxed and removed to a designated area under the supervision of the Medical Records staff, Nursing Director, Clinical Director, or designees, and by available staff.

- If removal of any hard copy confidential records or electronic media is not possible, the Medical Records staff, Nursing Director, Clinical Director, or designees, will check that all cabinets, doors and windows are closed and locked.

- Once all records and electronic media that can be are removed, files will be stored at off-site locations as designated in the Emergency Preparedness Plan.

- Because QBH's medical record system is backed up in a cyber network, consumer care can be readily resumed immediately from any setting. See the MethodOne Disaster Recovery Information Sheet for further information.

- Billing information is saved to a web-based network and is retrievable from any location or workstation as well.

- Administrative records are retrievable from the back-up drives as long as these have not been damaged or lost during a disaster or fire. QBH's goal, in progress, is to establish most of these as web-based documents.

TESTING OF THE CONTINGENCY PLAN

- QBH's contingency plan shall be tested at least annually under the oversight of the Privacy and Security Officers.

- For medical records, see the EMR system's Contingency Plan, Emergency Operations Mode Plan and Disaster Recovery Plan.

- Documentation of testing shall be maintained by the Privacy and Security Officers. These records shall be maintained for six years beyond the original documentation. Reports of results shall be included in their reports to the Leadership Committee within the quarter following the testing; the report shall include any recommendations for revision to the contingency plan and its components.

EVALUATION

- This policy shall be evaluated at least annually (every 12 months +/- 30 days) and as needed based upon findings from testing or actual implementation of the plan. The Security and Privacy Officers shall collaborate to make recommendations for any changes to the plan which will be submitted to the Clinical Committee. Likewise, these Officers will report on testing and/or actual performance of the plan in quarterly reports as appropriate and at least annually in the form of an overall evaluation of the plan.

FORMS

All HIPAA related forms
MethodOne Disaster Recovery Summary Information Sheet

QUALITY BEHAVIORAL HEALTH, INC. **MAT DISCLOSING PHI TO A CONSUMER 'S PERSONAL REPRESENTATIVE**

GENERAL GUIDELINES

- The scope of the consumer's personal representative's (CPR) authority to act for the individual is derived from his/her authority under applicable law to make health care decisions for the individual.

- Where the authority to act for the individual is limited or specific to particular health care decisions, the CPR is to be treated as the individual only with respect to PHI that is relevant to the representative.

- The CPR is subject to requirements of a valid authorization as set out in QBH's policy for release of information.

- Who Is Recognized as a Personal Representative

    - Adult

        - ✓ A CPR is a person with a legal authority to make health care decisions on behalf of the individual. [Example: court appointed power of attorney]

    - Deceased

        - ✓ A person with legal authority under applicable law to act on behalf of the decedent or the decedent's estate and this authority is not restricted to health care decisions.

ABUSE, NEGLECT, AND ENDANGERED SITUATIONS

- A physician or other covered entity may use professional judgment to decide against the release of PHI to a CPR in the following instances:

    - It is not in the individual's best interest to release the information to the CPR; and

    - The physician or covered entity reasonably believes that the patient may have been or may be subjected to domestic violence, abuse, or neglect by the CPR, or that releasing the PHI to the CPR would endanger the individual.

- The physician must document his/her decision to not provide information to the CPR and must include justification or rationale for that decision in the patient record.

EVALUATION

- This policy shall be evaluated at least annually (every 12 months +/- 30 days) and as needed based upon findings from testing or actual implementation of the plan. The Security and Privacy Officers shall collaborate to make recommendations for any changes to the plan which will be submitted to the Clinical Committee. Likewise, these Officers will report on testing and/or actual performance of

the plan in quarterly reports as appropriate and at least annually in the form of an overall evaluation of the plan.

FORMS

Release of Information Form
Authorization for Disclosure of Substance Abuse or HIV Information Form

PRE-ANNOUNCED AUDITS

- Notification is received by QBH that an audit has been scheduled or a need identified that requires production of consumer records for an off/on site audit.
- The CEO or Medical Director verifies that the external stakeholder requesting the audit has signed a Business Associate Confidentiality Agreement that mandates compliance with consumer PHI confidentiality.
- The Medical Records staff that receives the audit notification or records request will forward the notice/request to the Medical Director and CEO.
- Upon receipt of the notice/request, the Medical Director and CEO will notify all departments who will be involved in the audit.
- If necessary, the Medical Director and CEO will call a departmental or multi-departmental meeting to discuss the notice/request, coordinate, and assign tasks and dates of completion.
- The Medical Director and CEO will follow up with assigned staff regularly and report progress at the Clinical Committee meetings, if time allows.
- Upon completion of the audit, the Medical Director and CEO will coordinate the exit meeting to arrange for all applicable departments to have a representative at the exit meeting.
- Upon receipt of the information in the exit meeting, the Medical Director and CEO will notify all departments who need to be involved in the development of any required corrective action plan.
- If necessary, the Medical Director and CEO will call a departmental or multi-departmental meeting to discuss the corrective action plan, coordinate, and assign tasks and dates of completion.
- The Medical Records staff will remain present or available in the event the auditor/surveyor has questions or needs assistance.

UNANNOUNCED AUDITS

- When the CEO has confirmed the authenticity of the auditing organization and obtained a Business Associate Confidentiality Agreement (though this may be requested, it not required for JC as this agreement is already established via the survey agreement), s/he will await request for medical records from the auditing body's lead auditor/ surveyor.
- Once the type and number of records has been requested, the CEO and/or Medical Director will collaborate with the Medical Records staff to select the records to be pulled for audit.
- The Medical Records staff will pull the requested active and/or closed medical records, label each with the requirements that particular medical record meets and provide them to the auditor/ surveyor requesting the medical records.

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

- The Medical Records staff will remain present or available in the event the auditor/surveyor has questions or needs assistance.

EVALUATION/REVIEW:

- The CEO will review this policy annually and as needed and submit it to the Clinical Committee for review and approve.

FORMS

Business Associate Confidentiality Agreement

QUALITY BEHAVIORAL HEALTH, INC. **MAT FILING COMPLAINTS REGARDING PRIVACY OF HEALTH INFORMATION**

COMPLAINT RIGHTS

- Every individual has the right to file a complaint with QBH or the Secretary of DHHS concerning:
  - QBH's PHI/ePHI policies and procedures;
  - QBH's and/or a business associate's compliance with its PHI policies and procedures; or
  - QBH's compliance with federal privacy requirements.

SUBMISSION OF COMPLAINTS TO QBH

- Complaints must be submitted to the Privacy Officer (if PHI)/Security Officer (if ePHI), who is designated by law to receive complaints and answer additional questions.
- The complaint must be submitted in writing.

PROCESS FOR ADDRESSING COMPLAINTS

- The Privacy/Security Officer will review and investigate each complaint to determine if the complaint is valid and to identify an appropriate method for resolving the complaint. Investigation may involve interviews with the complainant, involved staff, policies review, observation or other methods appropriate to the nature of the complaint.
- In resolving the complaint, the Privacy/Security Officer will consider the individual's proposed resolution for the complaint.
- If at all possible the complaint shall be investigated and resolved with a written response to the complainant within 60 days of receipt.
- QBH will inform the individual in writing of the resolution of the complaint by the Privacy or Security Officer.

DOCUMENTATION OF COMPLAINTS

- QBH will document all complaints and the disposition of all complaints.
- QBH will retain all documentation related to complaints for six (6) years from the date the documentation was created.

SUBMISSION OF COMPLAINTS TO THE SECRETARY OF DHHS

- If an individual desires to file a complaint with the Secretary of DHHS, the individual must submit the complaint in writing to the following address:
  - At the HHS.gov website

- By mail to Secretary of U.S. DHHS, Office for Civil Rights, 200 Independence Ave. SW, Washington DC, 20201

- One may go to the website for more information about how to file a complaint www.hhs.gov/ocr/privacyhowtofile.html

- The individual must name QBH as the subject of the complaint and describe his/her complaint against QBH.

SPECIAL CONSIDERATIONS

- QBH will investigate all complaints and any other documentation containing credible information or evidence that QBH's workforce or business associates violated QBH's PHI/ePHI policies and procedures or the federal privacy requirements. QBH will appropriately resolve all such complaints and act on such information, as appropriate.

- QBH will not threaten, intimidate, discriminate, or retaliate against an individual who exercises his/her rights to complain to QBH or to the Secretary of DHHS.

EVALUATION

- This Policy will be reviewed by the Privacy/Security Officer annually and revisions made when necessary. The Policy will be forwarded to the Clinical Committee for review and approval when revisions are made and at a minimum of annually.

TRAINING

- The Privacy Officer/Security Officer will each conduct privacy and security training programs for QBH staff annually and as needed.
    - Privacy training will be conducted for new staff as part of QBH's general orientation program. General orientation shall consist of privacy and security regulation information with a general test of the information given at the end of the session.
    - The Privacy Officer/Security Officer will each conduct any specialized training programs for QBH staff related to the staff's particular roles in implementing QBH's privacy policies and procedures.

CONFIDENTIALITY AND SECURITY TRAINING

- Staff receives training at orientation and annually about the importance of confidentiality and security of any information related to our patients, staff and business documents. Staff training covers, minimally:
    - PHI, ePHI and IIHI definitions and what confidentiality practices are at QBH as regulated by HIPAA/HITECH.
    - What the civil and criminal penalties are for failing to protect PHI no matter what form it is in; personal accountability is emphasized.
    - Privacy Officer/Security Officer are introduced, their roles identified, and contact information is provided.
    - The procedures and timeframes for reporting unauthorized disclosures/breaches, virus or malware infection, need for maintenance or repair of electronic media whether Company or personally owned.
    - Informed that regulatory, accreditation and other governmental agencies can and will audit compliance and/or breaches, including the US Secretary or Health and Human Services or designee.
    - Instructed on procedures for disaster recovery and emergency mode operation in situations which might interfere with PHI/ePHI/IIHI security and/or access as appropriate to their job.
    - Instructed on Company policies and practices related to oral, paper and electronic security.
    - Trained in proper disclosure practices including when release is not required, when release is required, mandatory reporting, duty to warn reporting, what constitutes a legal release of information, minimum information necessary guidelines.
- Managers/administrators are additionally trained on their specific roles in reporting, record keeping required by HIPAA, investigation procedures as applicable to their job, Business Associate

Agreement requirements, and their specific roles in the security, disaster recovery, and emergency mode operations plans.

UPDATING PRIVACY/SECURITY TRAINING CONTENT

- The Privacy Officer/Security Officer and appropriate QBH staff shall be responsible to see that the content of the privacy/security training program is updated, as appropriate, to reflect any material changes in QBH's privacy and security policies and procedures. If material changes are made in privacy or security policies and procedures, QBH staff members whose work is affected by the changes shall be trained as soon as possible after those changes become effective.

DOCUMENTATION OF PRIVACY/SECURITY TRAINING

- QBH will document the privacy/security training conducted for its staff. Education and training provided to the staff shall be documented by attendance sheets and/or Virtual Center of Excellence training website reports. Training and test results are kept on file in Human Resources and in the staff's personnel file.

- QBH will retain for six (6) years all privacy/security training related documentation, including:

  - Attendance lists or Essential Learning reports for education.

  - Privacy/Security test results from privacy/security training in general orientation.

  - All written and/or electronic materials used for privacy training.

ANNUAL MANDATORY TRAINING

- QBH shall require annual review and testing of each staff on privacy and security requirements.

- Documentation of the annual mandatory training and testing shall be retained by the Human Resources Department and within staff's personnel files.

REMINDER POSTINGS

- The Security/Privacy Officer shall collaborate to design and oversee posting of posters and notices that provide prompts or reminders to staff on key privacy and security practices regarding both paper and electronic PHI.
-
  - These shall be posted at workstations in all offices/departments.

  - The Officer shall monitor that these reminders are still present during scheduled inspections and oversee replacement of any that are damaged or missing.

  - The Officer shall review these posters and notices at least annually and update as needed.

EVALUATION

- The Privacy and Security Officer will review this policy annually and as needed and revise when deemed necessary. Approval will be by the Clinical Committee.

FORMS

Release of Information Form
Authorization for Disclosure of Substance Abuse or HIV Information

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. MAT PRIVACY AND SECURITY OFFICER APPOINTMENT

PRIVACY OFFICER AND SECURITY OFFICER APPOINTMENTS

- QBH shall designate a Privacy Officer to oversee the development and implementation of QBH's privacy policies and procedures related to oral, visual and paper security, in accordance with applicable Federal privacy requirements. Likewise, a Security Officer is designated to oversee the development and implementation of QBH technological/ electronic security policies and procedures, in accordance with applicable Federal privacy requirements.

- It is the CEO's prerogative to have one person appointed who fills both positions.

SCOPE OF ACCOUNTABILITY

- The Privacy Officer shall be responsible for the development and implementation of QBH's privacy policies and procedures related to oral, visual, and paper privacy and for regular monitoring of staff's compliance with the related Federal privacy requirements.

- The Security Officer shall be responsible for the development and implementation of QBH's technological/electronic security policies and procedures related to all forms of electronic storage, transmission and/or receipt of personal health information and individual identifiable health information and for regular monitoring of staff's compliance with the related Federal privacy and security requirements.

- Each officer shall be the initial source for receiving immediate notice of any complaints, problems, or breaches in privacy information within the area of their accountability. Likewise, each is responsible to develop a report of any breach that they themselves discover during their compliance monitoring or that is received in the form of a complaint.

    - These officers are responsible to promptly inform the Chief Executive Officer.

    - These officers must always be part of the report and investigation process, as appropriate to their area of accountability.

    - Management of the investigation and resolution of any HIPAA related concern or complaint shall be by the appropriate officer, given the nature of the concern or complaint.

    - Both positions may be assigned to a single person due to the small size of QBH.

- Both officers shall be responsible for participation in internal investigation of any noted or reported breaches in management of privacy information (PHI, IIHI) or security of privacy information (ePHI) and shall engage as needed in any audits or investigations conducted by the Secretary of the US Department of Health and Human Services (HHS).

- Each officer shall provide education as needed to any assigned deputies, staff and/or managers related to their areas of accountability for privacy practices. Education, whether formal or informal, is included in quarterly reports to the Clinical Committee.

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

- Quarterly reports shall be submitted as calendared to the Clinical Committee (CC) describing, minimally, all activities and findings/trends related to testing of systems, compliance inspections, any unauthorized disclosures/breaches with any investigative findings or conclusions and status of each, any education provided, any recommendations for privacy system improvements and/or changes to policies or forms related to these systems.

    - The Privacy Officer's and Security Officer's specific duties shall each be defined in a job description. They shall be appointed and supervised by the CEO.

SELECTION

- The Privacy Officer and Security Officer appointments shall be approved by the Chief Executive Officer (CEO).

- The selection of the Privacy Officer and Security Officer shall consider each candidate's qualifications, educational background, work experience, and Clinical skills, including, but not limited to:

    - Knowledge and experience in health information privacy laws, access, release of information and information controls and security;

    - Knowledge in and the ability to apply the principles of health information management and project management;

    - Demonstrated Company, facilitation, communication and presentation skills;

    - Strong commitment to protecting the privacy of patients' protected health information.

    - The Security Officer shall have advanced experience with and knowledge of electronic security methods and with the EMR System, QBH electronic medical record program.

AUTHORITY OF THE PRIVACY OFFICER AND SECURITY OFFICER

- The Privacy Officer and Security Officer have the authority to enforce federal laws set forth by HIPAA, HICECH, FTC, and HHS as well as related state or accreditation requirements.

- The Privacy Officer and Security Officer each has the authority and responsibility to write up a report of the circumstances/observations of any violation of the confidentiality and/or security of confidential information by an employee, contractor or business associate of QBH and, if provided, a description of the immediate retraining done with the employee, contractor, intern, or business associate.

    - The original report shall be maintained in the staff's personnel file.

    - In the case of a violation by a business associate, the report shall be submitted by the Privacy Officer or Security Officer to the CEO who shall determine what course of action to take, which

may include a requirement of proof of retraining prior to further business affiliation with QBH, termination of the business association or other action deemed appropriate by the CEO based on nature/ severity of the violation.

- Each officer has the responsibility to initiate testing of and/or monitor the contingency plan and procedures for response to emergency or other threats to the areas of health information privacy within the scope of their areas of oversight.

- Each officer completes evaluations, at least annually, of the aspects of the privacy system for which they have accountability, considering any changes in federal and state regulations and/or environmental or operational changes affecting security of PHI/IIHI. They collaborate to arrive at any recommended changes in policy or forms.

EVALUATION

- The Privacy and Security Officers will review this policy annually and make modifications as needed based upon changes in regulations, changes necessary due to nature of services, etc. Any revisions will be submitted to the Clinical Committee as scheduled.

RELATED POLICIES/FORMS:

Confidentiality Affidavit Form
Personnel Handbook
Privacy Officer Job Description
Security Officer Job Description

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUARTERLY PROFESSIONAL REVIEW

- Quarterly review of records from all disciplines of QBH who document in the medical record shall be conducted by trained peers. No staff shall review their own records.
    - Review will include assessment of:
        - The quality of service delivery
        - Appropriateness of services provided
        - Patterns of service utilization
        - Consistent model implementation, where evidence-based practice is used, of key model components (e.g., frequency of service, specific curriculum, or protocols)

- Reviews are documented on the Peer Review Form appropriate for the discipline.
    - Data is aggregated by the Utilization/Quality Manager for each provider and by discipline.
    - Results are reported quarterly as scheduled to the Clinical Committee, using a code or ID number for each provider for confidential presentation.

THE REVIEW PROCESS

QUANTITATIVE REVIEW

- Medical Records staff conducts this medical record audit **monthly**. The review is documented on the *Medical Record Checklist*.

- A copy of the *Medical Record Checklist* is turned in to the Utilization and Quality Manager on the last workday of each month for aggregation and reporting, as scheduled within the quality system, to the Clinical Committee.
    - Trended reports are reviewed by the Committee quarterly to identify deficient areas that may need improvement.

QUALITATIVE REVIEW

- Monthly the Medical Records Clerk shall identify one record for each writer of a discipline (therapist, tech/monitor, nursing, and medical), and from each program (sub-acute, residential and outpatient), to be reviewed.
    - Each record will be one not previously reviewed.
    - Even months the records will be current, open records
    - Odd months the records will be closed ones, of consumers already discharged.

- The Medical Records Clerk will conduct the quantitative review on the selected records.

- The Medical Records Clerk will provide the medical record(s) to the contracted psychiatrist who will conduct the review of medical documentation.

- The Medical Records Clerk will provide the names of the records to be reviewed for the therapists and techs/monitors to the Clinical Director who shall delegate them to trained peer staffs to review.

- Reviews may occur from the hard copy of the medical record or from the electronic record, or from both, as appropriate and functional to the review being conducted.

ITEMS REVIEWED

QUANTITATIVE REVIEW

- Consumer medical record reviewed was:
  - Provided with an appropriate, documented orientation.
  - Actively involved in making informed choices about their services.
  - Had no information released or sought about them without completion of a Release of Information Form.

- Consumer assessments were completely filled out and were completed timely.

- Record components that are to be reviewed and updated per Company policy evidence timely review and/or update.

- For consumers being prepared for or who have been discharged, the transition plan and discharge summary are complete and done timely per Company policy.

- Services billed for a consumer match what services are documented in their medical record.

QUALITATIVE REVIEW

- Clinical, nursing and/or medical peer reviewers review for the following:
  - Assessments were thorough with all necessary information having been gathered or, if unavailable, an explanation is documented and the record evidence repeated attempts to gain the information from the consumer and/or guardian, previous provider or other appropriate informants.
  - Goals and objectives in the treatment plan were written based upon:
    - Needs evident from the assessment(s).
    - Included evidence of input from the consumer.
    - Revised when indicated.
  - Services provided were:
    - Related to the goals and objectives.
    - Consistent with those planned.
    - Of reasonable duration for the service provided.
    - Appropriate to the consumer's level of care.
  - Progress/service notes were documented in conformance to Company policy.

USE OF INFORMATION TO IMPROVE SERVICES

- Qualitative data is submitted to the Utilization and Quality Manager from the Medical Records Clerk. Completed Peer Review Forms are submitted within five days of having received directions to do the review. The Clinical Director shall collect these from staff and submit it to the Utilization and Quality Manager. Medical reviews are submitted to the Utilization and Quality Manager by the medical reviewer.

- Data from each month is aggregated and reported for the applicable quarter which also reflects results from previous quarters for each documenter using their assigned ID.

- Information collected is aggregated and reported to the Clinical Committee for analysis to identify trends that need attention, which may include:
    - Using the data to change processes and/or policies to improve service delivery.
    - Identifying the need for an improvement project to investigate a trend in more detail and then take appropriate action based upon the expanded data.
    - Using the data to identify need for additional training of individual staff or staff collectively.
    - Using the individual data for staff supervision and evaluation purposes.

- The trended and individual peer review records will be securely maintained in the office of the Utilization and Quality Manager.

EVALUATION

- This policy will be reviewed annually and revised as needed by the Privacy/Security Officer and submitted to the Clinical Committee for approval.

FORMS:

Peer Review Forms (by discipline)
Release of Information Form

QUALITY BEHAVIORAL HEALTH, INC. **MAT RECEIPT AND RESPONSE TO SUBPOENAS**

GENERAL GUIDELINES

- Some QBH contracts require staff to appear and give testimony regarding casework with consumers. Once received, the courts expect timely appearance, fully prepared to testify, whether subpoenaed by the state or by the defense.
- Subpoenas are common also for requests of medical records.
- Our policy is to comply with court expectations, to the extent possible, within the constraints of compliance with Federal HIPAA regulations in the exchange of information related to consumers served at QBH.
- By law the organization must respond to a subpoena, but the organization is not compelled to produce any information if valid grounds for objection exist, including a consumer's objection to the release of records or lack of a consumer's signed consent for Release of Information, unless Court Order or other law overrides the objection.

RECEIPT

- For consistency, all attorneys are encouraged to instruct their process servers to deliver all subpoenas to the CEO or acting administrator.
- Acceptance of court subpoenas is not a violation of a consumer's rights to confidentiality if QBH staff is being subpoenaed.
- If the subpoena is not generated at a QBH consumer's request, accompanied by a consumer signed Release of Information, or by a Court Order, QBH's attorney will have the subpoena quashed as a violation of HIPAA compliance.
- The receiving staff's response to a process server shall be," **I can neither confirm nor deny that this is about a consumer, but I will accept the subpoena because a staff's name is on it".**
- A subpoena that has been served directly to a QBH staff will be immediately submitted by the staff to the CEO.

VALIDATION

- The CEO or acting administrator will be responsible for determining if the subpoena is valid (meaning the appearance of a staff and/or records is in connection with a former or current consumer, has a signed consumer Release of Information or Court Order, and that the subpoena is signed and stamped by the Court Clerk or other tribunal if there is not Court Clerk).
    - If the subpoena is *not* valid, the CEO will consult with the Medical Director and a decision will be made on whether to notify the organization's attorney.

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

- If valid, the CEO will determine if there is sufficient time to have records copied, staff briefed, and still be in court at the appointed time.

  - ✓ If time is insufficient (i.e., providing less than a minimum of 10 days advance notice), the CEO or acting administrator may contact the issuing attorney's office to request a continuance be requested due to lack of sufficient response time.
  - ✓ If the attorney refuses, then the Medical Director shall be consulted, and a decision will be made on whether to notify the organization's attorney.

- The CEO will confirm that the subpoena is accompanied by a signed Release of Information from the consumer, unless there is a Court Order or there is evidence of reasonable attempt at consent accompanying the subpoena.

  - If there is no attached signed Release of Information from the consumer, the CEO or designee may contact the consumer to secure a written Release of Information.

  - If the consumer does not consent, their consent cannot be obtained, or it is otherwise determined appropriate, the organization's attorney will file an objection to the subpoena and the paperwork will be forwarded to the Medical Records staff to be filed into the consumer's medical record. A copy of the objection shall be mailed to the consumer at their last known address and/or to their attorney. A Court Order will be required to waive the objection, in which case, QBH must comply with the Court Order.

- The CEO shall also determine, in the case of subpoenas requesting information regarding QBH consumers who are receiving or have received substance abuse treatment services, whether the subpoena adheres to Federal confidentiality regulations mandated by 42CFR Part 2, "Confidentiality or Alcohol and Drug Abuse Consumer Records".

  - The Federal confidentiality regulation states, "If a person holding medical records subject to these regulations receives a subpoena for those records, a response to the subpoena is not permitted under the regulations unless an authorizing Court Order is entered. The person may not disclose the medical records in response to the subpoena unless a court of competent jurisdiction enters an authorizing order under these regulations." (42CFR, Part 2, Subpart E).

  - If the CEO or acting administrator receives a subpoena for information regarding a current or former substance abuse treatment consumer, they shall determine if there is an accompanying Court Order before responding to the subpoena.

  - If a Court Order is *not* present, the CEO or acting administrator shall contact the issuer of the subpoena and request that a Court Order be issued prior to making any disclosures requested by the subpoena.

- If it is determined that the subpoena is valid and there is sufficient time to respond, the subpoena will be submitted to the Medical Records staff for processing.

PROCESSING AND RESPONSE

- Consumer information release, in whatever form, shall comply with HIPAA regulations. See the HIPAA related policies for the entire process.

- The Medical Records staff keeps an electronic Records Disclosure Log to record any disclosure of consumer's confidential information that includes the consumer's name, the type of release, the day the record content was released, the nature of the data released, and to whom.

- Only Medical Records personnel, under the supervision of the Medical Records staff may release or disclose consumer information.

- If a consumer's medical record has been subpoenaed, and a signed Release of Information accompanies the subpoena, a copy of the subpoenaed information in the consumer record may be released, excluding psychotherapy notes. In the case of consumers who are receiving or have received treatment for alcohol or substance abuse, there must also be a Court Order for release of that type of information, in compliance with Federal regulation (42CFR, Part 2, Subpart E).

    - If the subpoena is presented to QBH with a Release of Information attached, the Medical Records staff will gather and copy the documents requested and, if time allows, will UPS the documents to the attorney or parole officer designated in the subpoena.

        - ✓ The documents may also be sent by certified mail or delivered in person.
        - ✓ The documents, together with an Affidavit of Custodian of Medical Records, shall be separately enclosed in an inner envelope and sealed with the title and number of the action, name of the witness, and date of the subpoena clearly inscribed thereon. The sealed envelope will be enclosed in an outer envelope, sealed, and directed to the Court Clerk or tribunal, if no Court Clerk.
        - ✓ A copy of the documents sent will be made and retained with the subpoena within the consumer's medical record.
        - ✓ Electronic copies shall not be used to satisfy a subpoena.
        - ✓ A bill shall be submitted to the requesting party for reasonable costs of production, pursuant to Michigan state law.

    - If the subpoena does not include a signed Release of Information, the subpoena and the paperwork, completed by the organization's attorney, as addressed earlier in this policy, will be filed into the consumer's medical record.

- The Medical Records staff will promptly follow the following steps when processing a subpoena:

    - The subpoena will be stamped with the date it was received.

    - If staff appearance is subpoenaed, the Medical Records staff will promptly notify the direct supervisor of the subpoenaed staff by phone and secure e-mail.

- ✓ The supervisor will notify the subpoenaed staff and arrange for consumer coverage, if needed, while the staff is making their appearance.

- The Medical Records staff will make a copy of the subpoenaed medical record and/or components and provide them to the staff that is scheduled to testify.

  - ✓ If there is not a Release of Information or Court Order for giving testimony, the staff, in conjunction with their supervisor, shall attempt to gain written consent from the consumer for the staff to give testimony, in which case the staff may answer questions as directed. If not, the staff may need to assert consumer confidentiality; however, the staff may be ordered by the judge to answer questions regardless of the assertion of consumer privileged communication, in which case the staff must answer questions posed.
  - ✓ After return from court, the staff who appeared in court will submit the medical record copies to the Medical Records staff for destruction; the time and date and documents destroyed will be noted on the HIPAA Records Destruction Log by the Medical Records staff once destroyed.

- Subpoenaed medical records (ONLY components subpoenaed) will be copied, by the Medical Records staff, for the court pursuant to the subpoena instructions. (Original medical records are NEVER provided to the court and DO NOT leave QBH and/or its archives.) The records will be accompanied by a notarized Affidavit of the Custodian of Records.

- If medical records only are subpoenaed, the Medical Records staff shall handle the copying and timely submission of those records requested (only requested records will be copied) once the subpoena is determined valid by the CEO or acting administrator and, when indicated, has the appropriate Court Order attached.

- The attorney sending the subpoena will be contacted by the Medical Records staff to confirm the subpoena was received.

- All subpoenas will be logged into the Subpoena Log. The following fields are completed:

  - ✓ Date the subpoena was received
  - ✓ Person requesting the information
  - ✓ Date the information was sent to the requestor
  - ✓ How the information was sent to the requestor (i.e. mail, faxed, hand delivered, picked up, etc.)
  - ✓ Description of the information disclosed.

- Any questions the Medical Records staff receives regarding the subpoena outside the scope of the medical record will be referred to the CEO.

- The official subpoena will be filed in the medical record of the consumer who initiated, or caused to be initiated, the subpoena.

EVALUATION

- This policy will be reviewed annually and revised as needed by the Privacy/Security Officer and submitted to the Clinical Committee for approval.

FORMS

Affidavit of Custodian of Records Form
Records Disclosure Log
Subpoena Log
HIPAA Records Destruction Log
Release of Information Form

QUALITY BEHAVIORAL HEALTH, INC. **MAT AUTHORIZATION FOR RELEASE OF HEALTH INFORMATION**

CIRCUMSTANCES WHEN RELEASE OF PERSONAL HEALTH INFORMATION AUTHORIZATION IS REQUIRED

- QBH shall release medical information only upon the receipt of a properly executed authorization from the consumer or the consumer's personal representative, or when permitted to do so by law and regulations. Only the Medical Records staff or CEO approved designee, may disclose or release PHI/ePHI/IIHI.

- Release requires authorization when:

    - Psychotherapy notes are requested, except when used to carry out treatment, for payment, for conducting health care operations such as quality management or peer review, for use by the originator, for internal training or supervision, and/or as defense in legal actions.

    - Used for marketing.

    - For the sale of PHI which is never allowed. A fee may be charged for the preparation and transmission of PHI for authorized purposes.

CIRCUMSTANCES WHEN RELEASE OF PERSONAL HEALTH INFORMATION AUTHORIZATION IS NOT REQUIRED

- Authorization is not required to release PHI in the following situations:

    - For release of consumer information to the consumer themselves or their legal representative. The legal representative must first provide proof of their position as legal representative.

    - To QBH's contracted Business Associates and their sub-contractors for purposes of carrying out their contract obligations.

    - When a consumer has been deceased for at least 50 years.

    - For treatment, payment and health care operations of QBH such as QA and I activities, UR activities and medical necessity reviews, resolution of internal grievances, etc.

    - For treatment of a consumer by a health care provider, including case management or care coordination or to direct alternative treatment or therapy.

    - For treatment by another health provider or setting of care.

    - Mandated disclosure of PHI such as for reporting of child or elder abuse, neglect or domestic violence; to the Secretary of HHS when requested; to public health authorities authorized by law to collect or receive such information; to track FDA regulated products and recalls; to legally authorized government oversight agencies; to the consumer's employer or school (not always mandated); to comply with a court order; in cases where criminal activity must be reported and/or investigated; to respond to a subpoena if authorization accompanies the subpoena or evidence of reasonable attempt is documented and included.

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. **MAT AUTHORIZATION FOR RELEASE OF HEALTH INFORMATION**

RELEASE OF PERSONAL HEALTH INFORMATION FORM

- The Form must be written in plain language a lay person would understand.
- The full Release of Information Form must be complete, or information cannot be considered for release. The Release must include:
    - Must designate to who (entity or person) the information is to be given and from who it is to be released.
    - Must include a description of the specific information to be used or disclosed.
    - Must include the name and signature of the person(s) giving authorization and, if not the consumer, then by what authority the person is signing. The authorizing signature should be compared with a signature on a photo identification card or against the medical record for authenticity.
    - Must provide a description of the purpose for the requested information. (A request from a consumer may simply state, "at the consumer's request.")
    - State an expiration date or event and not have been exceeded.
    - Must specify the consumer's name, address, and date of birth, and/or enough demographic information to properly identify the consumer. Be signed and dated by the consumer or the consumer's personal representative. (Personal representative must provide legal documents showing legal right to represent the consumer). If the release is coming from another person/entity, the authorizing signature should be compared with a signature on a photo identification card or against the medical record for authenticity.
- The individual's right to revoke the authorization in writing at any time and a description of how the individual may revoke the authorization.
- That release is not a condition for provision of treatment, payment or enrollment is so stated on the form.
- All Releases of PHI original signed authorizations shall be retained in the consumer's medical record. A copy is provided to the consumer/guardian. In an emergency circumstance where the consumer/guardian cannot provide authorization, QBH may disclose PHI necessary to emergency treatment, to a public or private entity assisting in disaster relief, or to the family in the case of death.

- The "Minimum Necessary Rule" shall be followed, which means when performing a task, only disclose the minimum amount of PHI/ePHI necessary. This rule applies to all with access to any element of PHI/ePHI, but does not apply to the PHI/ePHI exchanged between treatment providers. See the "Security, Confidentiality and Integrity Policy for further information on minimum necessary disclosures.

AGREED UPON RESTRICTION

- When a consumer is admitted to treatment they should be queried as to whether then desire any restrictions in disclosure or use of their PHI. If they do request restriction, the request should be submitted in writing, retained in their record, but a copy submitted to Medical Records or designees who might carry out release authorization requests. For example, a consumer might request restriction against release to a noncustodial parent or a family member prohibited from contact by the court, or a consumer living with a non-spouse might request restriction in information shared during a phone call to their residence.

- In some cases the restriction is mandated by law, such as the legal requirement not to release information about a consumer's substance abuse treatment.

- Any restriction placed legally or by the consumer prohibits the disclosure or use of their PHI in those circumstances.

DE-IDENTIFICATION OF PHI

- PHI that has been completely de-identified, meaning that it is not individually identifiable and cannot be re-identified by any logical or mathematical method (see the law for more details on de-identification) may be released without authorization. QBH may assign a code, symbol or other format to be able to re-identify the consumer for use internal to QBH only. See the Security, Confidentiality and Integrity Policy for further instructions.

EVALUATION

- This Policy will be reviewed by the Privacy Officer annually and revisions made when necessary. The Policy will be forwarded to the Clinical Committee for review and approval when revisions are made and at a minimum of yearly.

FORMS

Release of Information Form

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. MAT SANCTIONS, BREECHES AND INVESTIGATIONS

DEFINITIONS

Protected Health Information (PHI): individually identifiable health information, including whether an individual is in treatment or has died, that can be used to identify and individual, that is:

- Orally communicated;
- In hard copy format such as the traditional medical record;
- Transmitted by electronic media (ePHI);
- Maintained in any mode of electronic transmission, including the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using any type of storage media;
- Transmitted or maintained in any other form or medium.

Protected health information does not include:

- Education records covered by the Family Educational Rights; and
- Educational records, files, documents, and other materials which contain information directly related to a student and which are maintained by an educational Company or institution or by a person acting for such Company or institution; and
- Employment/contract records held by QBH in its role as an employer/contractor.

Privacy is the right of the individual to decide how much, to whom, when and in what manner personal information can be shared with others. Privacy is an essential ethical principle of mental health professionals, as well as a standard of care.

Use means sharing, employment, application, utilization, examination, or analysis of PHI/ePHI by the health professional or Company that maintains the PHI/ePHI. Use includes uses within the Company.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of PHI/ePHI by the health professional or outside of the Company holding the information. In some cases disclosure does not require prior authorization by the patient/guardian; in most cases such written authorization is required.

Minimum Data Necessary means that only that confidential information necessary to continuation/management of care shall be shared with another source, whether or not a release of information by the patient/guardian is required.

SANCTIONS FOR SECURITY INCIDENTS/BREACHES OF PRIVACY INFORMATION

COMPANY SANCTIONS

- Whether or not federal level action occurs, violations of confidentiality and security by an employee, contractor or business associate are grounds for corrective action up to and including immediate dismissal. Should a security incident/breach of privacy information occur, a report is submitted to the Clinical Committee by the Privacy or Security Officer who observed or received report of the incident; shall determine the sanction if anything beyond what the Privacy or Security Officer already carried out is determined necessary.

    - Clinical Committee's determination of sanction shall be based upon the risk associated with the circumstance and whether the violation is a repeat violation.

    - Actions with staff may entail, individually or severally:

UNINTENTIONAL INITIAL VIOLATION

- Verbal reprimand by the Privacy or Security Officer and immediate retraining on area of HIPAA/HITECH, FTC, HHS, JC confidentiality requirement that was violated. The reprimand is written up by the involved Officer as a warning; this documentation and documentation of the retraining shall be submitted to HR for inclusion in the individual's personnel file.

- Requirement for formal retraining in HIPAA/HITECH security and confidentiality policies and practices of the Company within 2 weeks of written notice from the Clinical Committee. Training should be arranged with the HR Manager. Documentation of the retraining must be contained in the individual's personnel file.

- Disciplinary action as set forth by Clinical Committee, which shall be documented in the individual's personnel file. Clinical Committee shall consider factors as addressed under federal sanction considerations in the following section of this policy.

Intentional and/or Repeat of a Prior Violation

- Intentional violation shall result in immediate job dismissal and report to the HIPAA Division of the Department of Social Security and to the Secretary of the US Department of Health and Human Services.

- A repeat of an unintentional prior violation may result in job dismissal at the discretion of the Clinical Committee after investigation is complete, depending upon the nature of the violation and the degree to which it created risk to consumers. Clinical Committee shall consider factors as addressed under federal sanction considerations in the following section of this policy.

FEDERAL SANCTIONS

- Any disclosure of unauthorized information is grounds for legal action at a federal level. There may be civil fiscal penalties and/or criminal penalties depending upon several factors. The type and amount of the penalty is accelerated for each violation. Civil penalties can range from $100 to $50,000 per violation, not to exceed $1,500,000 cumulative penalty per year.

- Violations where violator did not know or would not have known may be $100-$50,000 per violation, not more than $1,500,000 for identical violations in the same calendar year.
- Violations with reasonable cause without willful neglect may be $1000-$50,000 per violation, not more than $1,500,000 for identical violations in the same calendar year.
- Violations with willful neglect which is corrected within 30 days may be $10,000-50,000 per violations, not more than $1,500,000 for identical violations in the same calendar year.
- Violations with willful neglect not corrected within 30 days may be $50,000 per violation, not more than $1,500,000 for identical violations in the same calendar year.

- Factors considered in establishing a penalty include:
  - Nature and extent of the violation
  - Number of consumers affected
  - Time period during which the violation occurred
  - Nature and extent of harm resulting, including physical harm, financial harm, harm to a patient's reputation, hindrance to patient's ability to obtain health care
  - History of prior noncompliance
  - Whether attempt was made to correct any noncompliance
  - Response to prior complaints/investigations
  - Whether financial difficulties affected the provider/associate's ability to comply
  - Whether imposition of penalty would jeopardize the ability of the Company or business associate to continue to provide and/or pay for health care
  - Size of the provider entity or business associate.
- Criminal penalties, if determined to be indicated, are not issued by the HHS, but by a federal law enforcement Company and may involve imprisonment for six months or longer.

SECURITY INCIDENTS/BREACHES OF PRIVACY INFORMATION

COMPLAINTS OR DISCOVERIES – SUSPECTED OR KNOWN

- Anyone may report a complaint or a discovery of a security incident or of a breach with unauthorized disclosure of PHI/IIHI/ePHI to the Company or to the Secretary of the US Department of Health and Human Services (HHS).

- No one who files a complaint, testifies, assists or participates in compliance or investigation reviews, proceedings or hearings, or who refuses to do an unlawful act in an investigation may be threatened, intimidated, coerced, harassed, discriminated against or receive any other retaliatory action by the Company or its representatives.

- Whether a complaint is being filed with the Company or the HHS, the complaint must be in writing or submitted electronically, if secure, and include the name(s) of the person(s) who are the subject of the complaint, the date of suspicion or discovery, and the details, to the extent known, of the act or omission involved.

TO THE COMPANY

- If the complaint or breach is related to a Business Associate, they shall notify Chief Executive Officer (CEO) directly as soon as known or discovered but no later than 60 calendar days after discovery. Notification, by the CEO or designee, shall include written identification of each patient whose unsecured PHI is believed to have been accessed, acquired, used or disclosed during the breach and any other available information as it becomes available.

- If the complaint is by a patient or guardian, the complaint should be in writing to the attention of the Privacy and/or Security Officer, or, if given orally, shall be followed by a written complaint describing the circumstance under which they believe their privacy was jeopardized; the date when it occurred or was discovered; the staff involved, if known; and what they consider satisfactory resolution of the complaint. The receiving Officer shall promptly notify the CEO.

- If the complaint or discovery of a breach is by staff, it shall be reported IMMEDIATELY to the Privacy Officer (if the issue was with oral, visual or paper violations) or to the Security Officer (if the issue was of an electronic nature). The Officer shall promptly notify the CEO by phone or in person.

- All complaints shall be retained by the Company for a period of six years from the date of notice to the complainant of completion of and conclusions from the investigation.

TO THE SECRETARY OF DHHS

- The complaint must be filed by the complainant in writing or electronically to the Secretary of DHHS within 180 days of when the complainant knows of the act/omission, unless waived by the Secretary. The complaint must include the name of the person that is the subject of the complaint and a description of the act or omission believed in violation. A link is available on the HHS website.

MANAGEMENT OF COMPLAINTS, SECURITY INCIDENTS AND BREACHES OF PRIVACY INFORMATION

- Timeliness and thoroughness of investigation is imperative in these situations.

COMPANY INVESTIGATION OF COMPLAINTS OR DISCLOSURES

Investigation Activities

- The Privacy Officer and/or Security Officer shall do a preliminary review of the facts to determine if there is evidence to support an investigation and whether the violation, if it occurred, was a willful violation or not.

- The Privacy Officer and the Security Officer shall each keep a log of all alleged security incidents and complaints. The log shall identify, minimally:

  - What is the nature of the violation

  - The date it was discovered and, if it can be discerned, the date it occurred

  - The date the complaint or report of a security incident was received

  - The staff involved, if applicable

  - Whether or not a full investigation is indicated and, if so, includes the following:

    - ✓ The names of all consumers whose privacy information is involved
    - ✓ The extent to which any privacy information was accessed
    - ✓ An assessment of whether the source that accessed the information would what it was or what they could do with it
    - ✓ Whether any exposure occurred and, if so, how it has been used or disbursed, if possible
    - ✓ If any harm of any sort has occurred at the time of this investigation and prior to employment of mitigation activities
    - ✓ Date when mitigation activities, if applicable, were initiated and completed
    - ✓ Whether any notice outside the Company is indicated and, if so, what notice has been initiated, by what means, and on what date
    - ✓ Any other pertinent information

- While this initial exploration is to be documented on the log, a full investigation would <u>not</u> be necessary if, upon initial discovery, it is identified that one or more of the following situations exists:

  - Access or use was by another staff and was unintentional, made in good faith and does not result in further use or disclosure
  - It was an inadvertent disclosure by a staff authorized to access PHI/ePHI to another staff/person so authorized and the information received as a result of the inadvertent disclosure is not further used or disclosed

  - A disclosure where there is good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

  - Initial investigation supports a low probability that the PHI/ePHI has been compromised based upon a general risk assessment of 1) the nature and extent of information involved and likelihood of re-identification; 2) the unauthorized person who used or to whom the information was disclosed; 3) whether PHI/ePHI was determined to have been acquired or viewed; and 4) the extent to which the risk to the PHI/ePHI has been mitigated

- The Privacy Officer and/or Security Officer shall oversee initiation and implementation of a prompt investigation of the alleged complaint or breach if merited from the preliminary review. Every step of the investigation shall be documented in specific and clear detail by the Officer. Interviews shall be conducted as appropriate, reports and audits evaluated, equipment inspected as relevant, and all other actions necessary to ascertain if the complaint is founded and/or an unauthorized disclosure occurred and, if so, to what extent exposure occurred and to what degree there is risk of harm to consumers. The investigation shall be completed as quickly and as thoroughly as possible given the event and circumstances involved.

Mitigation Activities

- The Company, with oversight by the Privacy and Security Officers, shall conduct an annual risk analysis of potential risks/vulnerabilities to confidentiality, integrity and availability of PHI and ePHI, using the proactive risk analysis process. Findings from this analysis shall be addressed to minimize and/or eliminate potential vulnerabilities.

- To avoid harmful effects of violations in use or unauthorized disclosure, the Security and Privacy Officers will, promptly upon validation that a breach did occur, conduct a risk analysis to determine what may have contributed to this breach and action needed to prevent such a breach in the future.

- All mitigation activities shall also be documented by the Privacy and/or Security Officer and, if indicated, the IT Consultant.

Notification Activities – Written

- Should it be concluded that patient health information was inadvertently or willfully disclosed, patient(s) involved will be notified by the CEO or designee without delay and in no case more than 60 calendar days of the discovery. The notification shall be in plain language and shall include:

    - A description of what happened, including the date of the breach, if determinable, and date of discovery

    - A description of the types of unsecured PHI that was involved in the breach

    - Steps the patient(s) should take to protect themselves from potential harm because of the breach

    - A brief description of action taken to investigate the breach, mitigate harm to patient(s) and protect against further breaches

    - Contact procedures for patient(s) to ask questions or learn more, including a toll-free phone number, email address, Web-site or mailing address.

- Notice shall be written using first class mail to the patient at their last known address, or, if the patient agrees to electronic notice, by electronic mail. More than one mailing may be necessary as investigation reveals additional information pertinent to the patient. If the patient is known to be deceased, the notice should be sent to the next of kin or guardian.

- If contact information is insufficient or out of date, precluding written notification, a substitute form of notice calculated to reach the patient shall be used if the number of consumers involved is fewer than 10. If more than 10, the notice must be by conspicuous posting for a period of 90 days on the home page of the Website or in a major print or via broadcast media in a geographic area(s) where affected consumers likely reside. Notice includes a toll-free phone number that is active for at least 90 days.

- In cases where providing notice is deemed urgent, phone contact or other means may be used in addition to written notice.

Notification Activities – Media

- In cases where unsecured breach involved more than 500 consumers or a state or jurisdiction, prominent media outlets serving the state or jurisdiction shall be notified to issue an alert that includes a toll-free phone number consumers can call to gain information. Media notification shall be completed by the CEO or designee.

Notification Activities – Secretary of DHHS by the CEO or Designee

- If the breach involved less than 500 consumers, maintain a log of such breaches and, not later than 60 days after the end of the calendar year, provide notification as directed on the DHHS Web-site.

- If the breach involved more than 500 consumers, notification should be immediate and according to the instructions and using the forms available on the HHS Web-site.

Notification Restrictions – Law Enforcement Delay

- If the Company or Business Associate is notified by law enforcement that notification, notice or posting as required above would impede criminal investigation or cause damage to national security, the Company or Business Associate shall do the following:

    - If notification occurred in writing, delay for the time specified by the law official.

    - If notification was given orally by a law official, document the oral statement, including identification of the official making the notification statement, and delay temporarily but no longer than 30 days unless written notice is provided before the end of the 30 days.

Proof of Notification

- The Company and/or Business Associate, if applicable, have the burden of demonstrating that all notifications were made as required OR that the complaint and/or alleged use or disclosure of PHI did not constitute a breach.

INVESTIGATION BY THE SECRETARY OF DHHS

- An investigation is conducted much the same way as an audit or compliance review. One objective of this investigation is to determine if a violation occurred and, if it did, whether the violation was willful or intentional. The investigation may include any of the following and may occur onsite or offsite:
    - The Company or Business Associate will receive a written communication regarding the complaint, including a description of the act or omission that is the basis of the complaint, prior to initiating the investigation.
    - Review of pertinent policies, procedures, practices of the Company or Business Associate, as applicable.
    - Determination of circumstances surrounding the alleged violation.
    - Conduct of a compliance review of the Company's or Business Associate's records and required compliance reports/audits.
- The Company or Business Associate must:
    - Keep such records and submit them at such time, in the manner and containing such information as the Secretary requests
    - Cooperate with investigation and compliance reviews/audits
    - Permit access to information (if held by another entity, the Company must demonstrate and certify efforts to obtain the information)
    - Provide written testimony if so subpoenaed
- If the Secretary's conclusion is noncompliance, an attempt is made to reach resolution by informal means such as a demonstration of compliance or a completed corrective action plan. In this case resolution will be provided to the Company or Business Associate in writing.
- If not resolved by informal means, the Company or Business Associate will be given an opportunity to submit written evidence of any mitigating factors or affirmative defenses. These will be considered by the Secretary within 30 days.
- If, after review, the Secretary finds a civil penalty should be imposed, the Company or Business Associate will be informed. If no violation was found and no further action is warranted, the Company or Business Associate will be informed in writing.

EVALUATION

- This policy will be reviewed by the Privacy and Security Officers annually and revisions made when necessary. The Policy will be forwarded to the Clinical Committee for review and approval when revisions are made and at a minimum of annually.

FORMS:

Privacy Inspection and Security Inspection Forms

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

THE INFORMATION MANAGEMENT PROCESS

- The primary purpose for gathering and analyzing service delivery data is to assist Quality Behavioral Health, INC. in the following areas:
  - Strategic planning and other business decisions
  - Continuous quality improvement of services
  - Documenting compliance with all laws and regulations (Federal, State, CMH)
  - Maintain accreditation with JC
  - Reporting quantitative and qualitative data
  - Reduce redundancy and increase efficiencies
  - Development of longitudinal data
  - Analyzing Company performance
  - Appropriateness of services and associated costs
  - Analysis of resource use to enhance the cost effectiveness of care
  - QBH desires an increasing use of its management information system to foster a management culture based on "business intelligence".
- Quality Behavioral Health, INC.'s administrative team works in conjunction with staff to manage periodic MIS upgrades. The Chief Executive Officer, Clinical Director, and staff assess and select appropriate technology for QBH's needs. Periodically consultants are contracted to participate in technology needs assessment and upgrades. QBH will use technology in developing and implementing new services to maintain the competitiveness necessary for expanding services.
  - Additionally, QBH, Inc. does an internal assessment of technology use and needs at least ***every three years***. Focus of the assessment, conducted by the Clinical Committee, is on: 1) how well current technology works to enhance individual services; 2) the adequacy of current technology in improving the efficiency of staff; 3) any technological improvements needed to increase the productivity of staff; 4) how well QBH's technology works to facilitate communication with stakeholders; 5) what technology is needed to improve services to isolated populations, when applicable to QBH's programs; 6) whether there are sufficient phones, internet/intranet accesses, electronic resources, and tele-psychiatry resources to best serve any isolated populations served, if applicable.

ELECTRONIC DATA SYSTEMS

- As noted in the Recipient Rights Manual, all staff employed at Quality Behavioral Health, INC. is bound by Company standards and professional, ethical behavior which mandates a strict adherence to the requirements of consumer privacy and confidentiality. This requirement applies equally to all data collection processes. There are currently three electronic systems being utilized for data management:

CONSUMER TRACKING AND BILLING (CT&B)

- **CT&B System:** As required by the Macomb County, consumer data is collected which contains demographic, diagnostic, treatment, and financial information. In addition, Macomb County require that this data be submitted to them on a regular basis. Regular reports are created and appropriately distributed. Access to this data is available only to QBH staff involved in the process of complying with Macomb County Community Mental Health Company mandate of forwarding the data. Data transmitted to them is entitled by HIPAA required 837 formats and is received by an https site secure socket layer web site at each organization.
- Training for the Reimbursement Specialists is provided by Practice Management Technology on an

as needed basis. The QBH staff is trained on the CT&B system by the Systems Manager or Reimbursement Specialist(s).

- Additionally, any coding training which becomes available will be attended by the Clinical Director, the CEO, the Utilization and Quality Manager, the Accountant, and the Systems Manager. The information obtained will be disseminated to all staff.

QUALITY DATA SYSTEM

- The results of all data collected by the Utilization and Quality Manager having to do with findings from monitoring and evaluation. These are maintained in the Utilization and Quality Manager's office computer; the G drive and hard copies of aggregate data are distributed to appropriate staff and the Clinical Committee.

ELECTRONIC RECORD SYSTEM SOFTWARE

- The Administrative Assistant /Office Manager sets the security for all those persons who have access to the Electronic Medical Record System: Sigmund Software. The security is set using a password and special menu selection. Only information pertinent to the staff person will be available. Permissions will be established by the Utilization and Quality Manager at the direction of the Clinical Director. Each staff person can access and retrieve data without breaching security or confidentiality. Staff profiles are removed upon termination.

- For sites using the Electronic Medical Record Software (Sigmund Software) program:
  - The computer system has several levels of security to maintain confidentiality and data integrity.
  - Only clinically privileged, appropriately designated administrative, or designated support staff are given complete access to complete stored clinical data.
  - The system does automatic back-ups which are held in the cloud perpetually.
  - Additionally, a pdf back-up of each record is retained in a fire retardant and waterproof, locked cabinet within the locked file room. The Clinical Director and Medical Records Coordinator are the only persons with a key to this locked file.

- QBH does not currently have a network server system on- or off-site for any other types of documents.

CONFIDENTIALITY AND SECURITY

COMPUTERS, I PADS, TABLETS AND NOTEBOOKS

- Security to Company computers occurs on two levels. The first is the operating system password that gives access to the file server where the consumer data files are stored. Only individuals with privileges or rights to the stored device (e.g., drive G) are allowed to access these files. This is set by the system administrator under the supervision of the CEO or Administrative Assistant/Office Manager. Secondly, within the electronic clinical record a second password is established that allows access to the Sigmund Software program. Access to clinical records is established by staff position under the following categories:
  - Primary Clinician/Therapist - Refers to caseload or individual records assigned to a given clinician or on a need-to-know basis.
  - Case Manager - Refers to individual cases assigned to a case manager across programs.

- Monitors – Refers to paraprofessional staff that assist clinicians in treatment implementation and milieu maintenance for access only to specific documents.
- Clinical Director and Physicians - Refers to entire programs (one or more), assigned to a supervisor and/or physician, giving them the access to all cases assigned to those programs.
- Administrative / Clerical - This level of security only gives a clerical or administrative staff access to schedules, not clinical information.
- Administrative Assistant/Office Manager - This level of security gives a user access to all system functions, clinical data and configuration settings. This level of security is offered only to the system administrator or the highest-level administrators / managers.

- All passwords are to be kept confidential. Sharing of passwords and other such security information is strictly prohibited. Computer users are encouraged to use passwords that are at least 7 characters long. Individual passwords are to be changed every 30-45 days.

- QBH's wide area network can also be accessed by remote users. This is accomplished by the use of remote configuration of terminal emulation software that uses industry standard SSH tunneling into QBH's virtual private network. Special arrangements are made within system administrator to gain access to this system. The remote user must be issued a remote version of the software, given the menu password to gain access. In the event a staff member terminates employment an immediate suspension of access to QBH network is invoked by the Administrative Assistant /Office Manager.

HARD COPY CONSUMER MEDICAL RECORDS

- QBH's hard copy consumer medical records are kept in locked file cabinets in a locked Medical Records storage area when they are not in use. It is the policy of QBH to maintain the confidentiality of consumer records.
  - To facilitate security of all consumers' medical records, each site has a separate file room to store and maintain records.
  - At each site there is a primary and alternate person identified who is responsible for overseeing that consumers' records are kept confidential. If both the primary and alternate individuals are off from work at the same time (vacation or personal leave), they will designate a temporary replacement to maintain the security of QBH consumer medical records.

INTERNET

- Internet is available at QBH, Inc. on a 24/7 basis. However, the internet may be accessed only by designated staff, including all clinical staff, except for monitors, and the CEO.

- Confidentiality guidelines follow as for other electronic media. Those allowed access to the internet are assigned a password by the CEO or Administrative Assistant/Office Manager.

EMAIL

- Email sent from QBH electronic, or phone equipment may not be used to solicit others for commercial ventures, religious or political causes, outside organizations or other non-business matters.

- Emailing of any non-encrypted identifying consumer information (PHI) or any non-encrypted staff/employee identifying information (PHI) to external organizations is prohibited.

- In the event it is necessary to send consumer or staff identifying information via email, this information/data will need to be encrypted and password protected as follows:

- Create the document in Word or Excel; save and close the file.
- Create an email document; proceed to insert icon and click on "Attachment."
- Proceed to "My Documents" and locate the document; click on the document.
- Right click on the document and select "AXCRYPT"
- Enter a password of your choice and LOCK the document (this process has now password protected your attachment).
- Proceed to send the email; send the password to the intended receiver via other methods (phone, fax, text message).

FACSIMILES

- Facsimiles are the responsibility of all support staff to distribute to the appropriate person(s).

- Incoming and outgoing facsimiles are not to be left unattended nor remain on or near the fax machine under any circumstances.

- Fax machines are in secure settings. The Administrative Assistant will secure all incoming facsimiles for administrative staffs.

COMPANY CELL PHONES

- Any cell phones used for and/or storing Company information are to be password secured. The Administrative Assistant keeps a secured list of passwords for those to whom Company cell phones are distributed.

TEXT MESSAGING

- Computer, phone, tablet, iPod, I Pad, notebook or other electronic text messaging of a care recipient's, staffs or business information is discouraged, but when used, it must comply with the de-identification directives that follow. In no circumstances should information below be included via these media. Non-compliance with this policy may result in disciplinary action and/or contract termination as it is a component of HIPAA compliance. De-identification of protected health information for communications necessary for staff to fulfill their duties includes elimination of the following list and/or submission of ONLY password protected texts or emails when staff or patient information is involved.
- QBH may determine that health information is not individually identifiable health information if the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed/not included: 1) Names; 2) Address; 3) Telephone and fax numbers; 4) Electronic email addresses; 5) Social security numbers; 5) Medical record numbers; 6) Health plan beneficiary numbers; 7) Account numbers; 8) Certificate/license numbers; 9) Vehicle identifiers and serial numbers, including license plate numbers; 10) Internet Protocol (IP) address numbers; 11) Biometric identifiers, including finger and voice prints; 12) Full face photographic images and any comparable images; and 13) Any other unique identifying number, characteristic, or code.

WEB BASED DATA

- All web-based data is sustained in a secure fashion consistent with the nature of the web source.

- An IT person is available, by agreement; the IT person assists with internet/electronic communications problems as needed.

VIRUS PROTECTION

- QBH uses commercially available virus protection programs; typically, MacAfee or Norton virus protection software is used.

- Only the Utilization and Quality Manager is allowed to utilize a USB for back up of quality and utilization system data. All other back up, as described elsewhere in this policy, is web-based or network-based. The Utilization and Quality Manager and other staff required to store sensitive data utilize a True crypt system that encrypts all or sections of data on the computer, I pad, tablet or USB. This system also is password protected.

DATA DEFINITION AND METHODS FOR CAPTURING DATA

- **CT&B System:** Data collection is done on dedicated computers in which the program is contained. This software has significant data validation; however, it is impossible to prevent data entry errors. The data collected is identical in nature to that collected by all agencies contracted with the Macomb County Community Mental Health Company which allows for comparisons in the aggregate across the system.

- **Quality Data System:** Data collection in this system is conducted by the Utilization and Quality Manager and Clinical Committee. The nature of this data is defined in the *Quality Management Plan.* The software program will provide greater assistance in the capture and analysis of all data for quality purposes. While the specific information elicited from this system is unique to QBH, the essential issues it monitors are universal across similar agencies.

- **Electronic Consumer Records:** Medical Records staff routinely review the charts to monitor for the presence, timeliness, and signatures of, but not exclusively, the following:
  - Consent to treatment
  - Fee Agreement
  - Your Right to Confidentiality (acknowledgement of receipt of Recipient Rights information)
  - Recipient Rights Notification Form, including The Fair Hearing and Second Opinion
  - Consumer Self-Assessment or Person-Centered Assessments (Case Management, Comprehensive or Psychosocial, Social Functioning, Nursing Assessment, Health Assessment)
  - Copy of the Insurance card
  - Treatment Plan / Service Reviews (Status Reports)
  - Psychiatric Evaluation
  - Tardive Dyskinesia Evaluation
  - AIMS test
  - Consent for Treatment with Psychiatric Medications

ASSISTIVE TECHNOLOGY

- Various resources are available for staff requiring assistance to use the technology available at QBH, Inc. These include:
  - Dragon, a program for the motor impaired that allows the person to speak and the computer

types what is spoken, is available on most computers.
- All computers and I Pads have speak and read capability for the visually impaired.
- Some computers and I Pads have a braille encrypted keyboard for the visually or hearing impaired.
- Adaptive phone is available at the Detroit and Gratiot offices that will read, do talk to text, have volume adjustments for the hearing impaired, and lighting adjustments for the visually impaired.
- Touch screen computers are available to those who cannot operate a mouse.

STAFF TRAINING ELECTRONICS

- There are tablets (at the Sterling Heights offices) with eBooks that contain training documents and CPT codes that are available to clinical staffs.

- Virtual Center of Excellence website is used for staff training. Each individual training program is followed by a test. Staff gets an alert when training is do or needs to be repeated. Reports can be generated for HR as needed. The system is accessible from anywhere and is available to all Mental Health Programs providing services within Wayne Co. The program is a resource provided by the Wayne County District MH Company.

ELECTRONICALLY SENSORED DOORS

- All main entries to facilities, the CEO's office, all clinical record file rooms, and all clinical area entry doors are sensor operated.

- Sensors are tested by Security Team members at least every other month and as needed.

REMOTE COMMUNICATIONS TECHNOLOGY

- No interactive technology is available to communicate with consumers, other providers or their families, such as tele med or similar electronic technologies at this time.

- QBH does use Skype and/or DropBox to communicate between the CEO and various staffs and/or QBH's consultants. Patient information is not exchanged in Skype communications. Skype communication can occur either by computer or cell phone.

DISSEMINATION OF DATA

- Quality Behavioral Health, INC. submits data to Macomb County Community Mental Health Company regularly. Reimbursement Specialists use the export utility from CT&B to compile the information that is submitted. Monthly reports are given to directors. The reports are set so that they can retrieve information in a short period of time. Some reports contain consumer statistics, event and billing data.

- Information from the Quality Data System is generated on a regular basis and maintained by the Utilization and Quality Manager. As appropriate, data is provided to the Chief Executive Officer, Clinical Director, and others, as needed. All aggregate data is reported to the Clinical Committee as scheduled.
- QBH increasingly strives to be a data driven organization. Results and recommendations are summarized for the Board of Directors on a regular basis.

COORDINATING DATA INFORMATION

- The rationale for all data collection is to continuously improve the quality of services provided. This enables QBH to link consumer care and non-consumer care data and information, both internal and external, over time. Currently, the systems utilized at QBH do not enable us to make information available from the MIS to the Quality Data System electronically. It is a goal toward which this Company is striving so that we will:
  - Provide and access longitudinal data and information
  - Organize data effectively, interpret and clarify it
  - Analyze situations based on this data
  - Make decisions based on this analysis
  - Continuously review the process, system, and outcomes to improve services and customer satisfaction
- A search is underway to determine how to coordinate data generated on I Pads, Notebooks, Tablet and Laptops with the main hardware system, using a shared network, for all QBH owned electronics

MEDICAL RECORDS

(See also the Consumer Medical Record Policy)

- QBH's intake process begins on the phone or at the front desk when the consumer makes their first visit. The consumer receives a packet of information that includes rights and confidentiality advice, consents for treatment and medications, insurance forms and other items for use at QBH. The clerical staff makes copies of insurance cards and licenses. The consumer then sees a counselor and the Reimbursement Specialist. At this time a doctor's Psychiatric Evaluation appointment is made for the consumer, if applicable to that program. The consumer registration form is given to the Reimbursement Specialist for processing.
  - We do request that our consumers provide us updated address, telephone, insurance, or other changes so that the MIS system can be frequently updated. The Medical Records Manager reviews records daily for completeness, uniformity, and signatures.
- Each consumer who has been assessed, treated, or served at QBH has a medical record which incorporates information about all these services. Only direct care staff may make entries in consumer medical records. Clerical staff responsible for scheduling appointments and financial matters may also make entries for these purposes. Entries and information are expected to be included in the chart as soon as possible after the event being recorded, dated, and authenticated. The case file should contain sufficient information to:
  - Identify the consumer
  - Support the diagnosis
  - Justify the treatment
  - Provide documentation for the course and results of treatment accurately
  - Facilitate continuity of care among health providers.
- After discharge, consumer medical records are maintained in separate locked files for closed medical records.
- All entries into medical records must be dated and signed with the appropriate credential. QBH maintains a list of all current staff signatures and credentials for the purpose of signature verification, if necessary.

EXTERNAL INFORMATION SOURCES AND COMPARATIVE DATA

- As described above, aggregate data is obtained from both internal and external sources. The information is utilized to support management decisions and operations, performance improvement activities, and care delivery. Tracking trends over time is also possible particularly in the case of the Quality Data System.

- With the utilization of M-Link and other Online Databases, it will be possible to review other up-to-date sources for clinical and management literature, reference information and research data.

MEDICAL, BILLING, ACCOUNTING AND QUALITY RECORDS RETENTION AND DESTRUCTION

- All information is stored in a secure manner (e.g. locked cabinets, or by password security if in computerized format).
- Consumers' record information is stored in paper (hard copy) format for 7 years for all consumers. Corresponding activity information is stored for one fiscal year. All electronic media is maintained indefinitely. Consumer medical records are destroyed by shredding or placing in the shredding bins and performed by the appropriate contractor when necessary.
- All "aged" (according to above) or extraneous information is to be shredded by individuals or by Medical Record staff.
- Accounting information, reports and data are maintained for 7 years. Audit information is retained for 15 years.
- In the event any legal process initiated against the organization, the CEO or designee will immediately secure the pertinent information to prevent any malicious destruction of the records. Any unauthorized person found destroying information could be subject to immediate termination or legal proceedings.
- Destruction of data is prevented by means of electronic back-up media which is maintained on and off site. This back-up media is only available to authorized staff persons.

DISASTER RECOVERY

- Daily back-ups are created with a full back-up locked in QBH safe and a second copy kept off site.
- In the event of a location disaster off-site data will be restored at a secondary location. This will be done by using a portable back-up device (e.g., parallel port DAT Drive).
- Disaster Recovery software will be purchased and updated as needed.
- Full Security Assessments will be contracted periodically, and weaknesses addressed.
- An **annual** mock disaster situation will be created, and recovery activities will be tested.

TECHNICAL ASSISTANCE

- If difficulties arise with software, the technical assistance available from the software company is utilized.
- If difficulties arise with hardware, an outside resource is consulted to determine if the hardware is repairable and at what cost. The CEO then decides whether to repair the hardware or dispose of it and replace it.

SOFTWARE SYSTEMS

- The following software packages are currently in use by QBH:
  - Sigmund Software Package
  - Microsoft Office 365

- QuickBooks Accounting Software
- McAfee and Norton Antivirus Software
- TrueCrypt Software

TESTING AND DEPLOYMENT

- When new systems, hardware or software are implemented, a phase in testing period is initiated. New systems are deployed prior to eliminating existing systems. Depending on the importance of newly implemented software, parallel systems will be maintained for at least 30 days.
- When new systems have reached a satisfactory threshold of performance as outlined by system vendors, they are then allowed to go "live" for permanent and full-time utilization.
- Whenever possible hardware and software solutions are installed with as much redundancy as possible given available technology and financial resources.

TECHNOLOGY GOALS FOR 2020-2021

- Develop connections to make information available from the MIS to the Quality Data System electronically.
- A search is underway to determine how to coordinate data generated on I Pads, Notebooks, Tablet and Laptops with the main hardware system; exploring Microsoft Sheer Port File Sharing System.
- Linkages to up-to-date sources for clinical and management literature, reference information and research data.
- An efficient and cost-effective means for uploading hard copy/handwritten documents of the medical record into the electronic record.
- Scan all closed and open medical records into the electronic medical record system going back 7 years.
- Non-transportability of some software some computers exists due to aged out and non-compatibility with software; from now forward, all computers are to be of same brand with the same hardware, programming, memory, etc. characteristics

ANNUAL REVIEW

- The Technology Plan and goals will be reviewed annually), or as needed and revised by the Clinical Committee to ascertain progress, identify new goals, and to update the plan if needed.

FORMS:

None

MEDICAL RECORD PEER REVIEW
COUNSELOR FORM
QUALITY, ACCURACY, AND COMPLETENESS

LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #	
RECORDER INITIALS	

ASSESSMENT

INTAKE AND CLINICAL ASSESSMENT THOROUGH

ITEM	CODE	COMMENTS
CONSUMER IDENTIFICATION DATA COMPLETE		
MENTAL/SOCIAL HISTORY: a. PRESENTING PROBLEMS		
b. DETAILS OF PAST AND PRESENT ADDICTIONS (DRUG/ALCOHOL/NICOTINE/OTHER) INCLUDES MINIMALLY: - Age of onset - Method of acquiring substance - Duration - Patterns of use (for example, continuous, episodic, binge) - Frequency, amounts, and route of the substance that is taken		
c. SUICIDE RISK SCREEN IS COMPLETE		
d. SUICIDE RISK ASSESSMENT IS COMPLETE (if suicide screen indicates consumer is at risk)		
e. SUICIDE RISK REASSESSMENT IS DONE AT EACH TREATMENT TEAM REVIEW (if consumer is a suicide risk)		
f. RELEVANT PAST SOCIAL//LEGAL/MILITARY HISTORIES COMPLETE		

MEDICAL RECORD PEER REVIEW
COUNSELOR FORM
QUALITY, ACCURACY, AND COMPLETENESS

LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #	
RECORDER INITIALS	

ITEM	CODE	COMMENTS
g. RELEVANT PAST FAMILY HISTORY (APPROPRIATE TO AGE)		
h. CD HISTORY COMPLETE		
i. PAST TX COMPLETE		
j. EDUCATION/VOCATIONAL HISTORY COMPLETE		
k. SCREEN FOR TRAUMA, ABUSE, NEGLECT, AND EXPLOITATION COMPLETE AND ASSESSMENT (if applicable) COMPLETE		
l. MASTER PROBLEM LIST CORRECTLY DONE AND CURRENT: INCLUDES **ALL** NEEDS/ISSUES WHETHER TREATABLE AT THIS AGENCY OR NOT		
m. STATEMENT OF CONCLUSIONS OR IMPRESSIONS DRAWN FROM THE PSYCHOSOCIAL HISTORY		
n. OTHER CLINICAL ASSESSMENTS DONE IF INDICATED		
o. CENTRAL REGISTRY VERIFICATION DOCUMENTED (unless done by MD or Nsg.)		
MULTIDIMENSIONAL ADMISSION ASSESSMENT (STATE FORM) THAT DETERMINE THE APPROPRIATE LEVEL		

MEDICAL RECORD PEER REVIEW
COUNSELOR FORM
QUALITY, ACCURACY, AND COMPLETENESS

LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #		
RECORDER INITIALS		
OF CARE IS IN RECORD (if LOC objection, it is documented in consumer record) if not done by MD		
SUMMARY INTEGRATING ASSESSMENTS		
DIAGNOSIS OR DIAGNOSTIC IMPRESSION		
TREATMENT PLANNING		
ITEM	**CODE**	**COMMENTS**
PLAN GOALS AND OJBECTIVES ADDRESS CONSUMER'S NEEDS AND PREFERENCES		
STATEMENT OF COURSE OF ACTION PLANNED FOR CONSUMER		
SMOKING AND TABACCO CESSATION ARE INCLUDED IN THE TREATMENT PLAN (if applicable)		
EDUCATION AS TO THEIR RISK, OVERDOSE PREVENTION EDUCATION, AND PROVISION OF NALOXONE IS PART OF TREATMENT PLAN (for consumers on benzodiazepines, even by prescription)		
GOALS AND OBJECTIVES • RELEVANT TO DIAGNOSIS AND SYMPTOMS • REVISED WHEN INDICATED		

MEDICAL RECORD PEER REVIEW
COUNSELOR FORM
QUALITY, ACCURACY, AND COMPLETENESS

LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #		
RECORDER INITIALS		
TREATMENT IS APPROPRIATE TO LEVEL OF CARE		
TREATMENT IS REVISED AS NEEDS CHANGE AND WHEN INDICATED		
ITEM	**CODE**	**COMMENTS**
PROGRESS NOTES		
NOTES REFLECT CLINICAL OBSERVATIONS AND RESULTS OF THERAPY		
NOTES REFLECT COUNSELING SERVICES PROVIDED AS IN TREATMENT PLAN		
NOTES REFLECT SERVICES OF REASONABLE DURATION FOR NATURE OF SERVICE PROVIDED		
REFLECT SERVICE APPROPRIATE TO THE CONSUMER'S LEVEL OF CARE		
DOCUMENTATION SHOWS CONSUMER RIGHTS ARE PROVIDED AT INTAKE/END OF TRANSITION/IF RIGHTS LIST CHANGES		
SERVICE PROVIDED RELATES TO CONSUMER'S TREATMENT GOALS AND OBJECTIVES		

MEDICAL RECORD PEER REVIEW COUNSELOR FORM QUALITY, ACCURACY, AND COMPLETENESS *LEGEND: Y = YES N = NO NA = NOT APPLICABLE*		
MEDICAL RECORD #		
RECORDER INITIALS		
NOTES ADDRESS CONSUMER RESPONSE/PROGRESS IN TX		
FINAL DIAGNOSIS(ES) OR DIAGNOSTIC IMPRESSION(S)		
CONCLUSION AT TERMINATION OF CARE/SERVICES		
DISCHARGE SUMMARY		
AFTER CARE FOLLOW UP (IF CLOSED RECORD)		

NOTE: The Quality and Utilization Manager will randomly select at least 3 records for each practitioner for review by another like-type practitioner during each quarter, using the peer review form appropriate to that discipline. Completed reviews are to be submitted to the Quality and Utilization Manager by the deadline communicated when the reviewer was notified which records to review and for which practitioner.

MASTER PROBLEM LIST

DATE IDENTIFIED	PROBLEM	INITIAL STATUS*	CHANGE IN STATUS **
	SUD:		
	Health:		
	Mental health:		
	Housing:		
	Education/Employment:		
	Family:		

***Initial Status Options:** Active, Referred, Deferred
****Change Status Options:** Resolved, Cancelled, Deferred, Referred

CONSUMER SIGNATURE

COUNSELOR

Initial: ____(/ /) 90 Day Review: ____(/ /) Annual: ____(/ /)

QBH ABBREVIATION AND SYMBOLS

A	
a (line over a)	before
AA	Alcoholics Anonymous
Abd	abdomen
ACT	Assertive Community Treatment
a.c.	before meals
ADHD	Attention Deficit Hyperactivity Disorder
ADA	Diabetic Diet
ADD	Attention Deficit Disorder
ADL	activities of daily living
ad lib	at pleasure; as desired
adm	admission
ad noct	at night
ADS	Abbreviated Dyskinesia Rating Scale
AEB	as evidenced by
AIDS	Acquired Immune Deficiency Disorder
alc	alcohol
A.M.	morning
AMA	against medical advice
amb/AMB	ambulatory / ambulation
amt	amount
Appt.	Appointment
A.S.A.	aspirin
ASAP	as soon as possible
attn	attention
B	
BC/BS	Blue Cross / Blue Shield
bid	twice a day
bio	biological
BM	bowel movement
BP	blood pressure
BPD	Borderline Personality Disorder
BR	bedrest
Bro (line over o)	brother
BSN	Bachelor of Science in Nursing
Bx	Behavior
C	
C (with line over)	with
cap.	Capsule
CBC	Complete Blood Count
chol.	Cholesterol
chr	chronic
Clt	client
cm	centimeter
C&S	culture & sensitivity
CNS	central nervous system
c/o	complains of
cont.	continue treatment

CPR	cardiopulmonary resuscitation
CSW	Clinical Social Worker
D	
D.A.W.	dispense as written
dept.	department
dev	development
D/C	discontinue
dx.	diagnosis
Dir	Director
Disch.	Discharge
D.M.	diabetes mellitus
doc	document / documented
DOB	date of birth
Dr.	doctor
DS	discharge summary
Dsg	dressing
DX	Diagnosis
E	
EEG	electroencephalogram
EKG/ECG	electrocardiogram
ENT	ear, nose and throat
ER/ED	emergency room/department
ETOH	ethyl alcohol
exam	examination
Exec.	executive
ext.	external
expl	explore
F	
F	Fahrenheit
Fa	father
FHx	family history
FNP	Family Nurse Practitioner
freq	frequency
ft	foot
F/U	follow up
G	
g	grand (for grand mother, grand father)
gal	gallon
gen	general
Gen Med	general medicine
GI	Gastrointestinal
gm	gram
gro	group
gtt/ott	drop
GU	genitourinary
GYN	gynecology
H	
H_2O	water
HBV	Hepatitis B Vaccine
HEENT	head, eyes, ears, nose, throat
HIV	Human Immunodeficiency virus
hr	hour
hrs	hours

ht	height
Hx	history
hyst.	hysterectomy
I	
IBW	Ideal body weight
IEP	individual educational plan
Ind	individual
IM	intramuscular
I & O	intake and output
IP	inpatient
K	
Kg	kilogram
L	
L	left
lab.	Laboratory
lb.	pound
LCSW	Licensed Certified Social Worker
LICSW	Licensed Independent Certified Social Worker
LMHC	Licensed Mental Health Counselor
LMP	last menstrual period
LOA	leave of absence
LOC	level of consciousness
LPN	licensed practical nurse
LSW	Licensed Social Worker
M	
MA	Master of Arts
Mcg	microgram
MD	Doctor of Medicine
Med.	Medicine
Med	Master of Education
mEq	milliequivalent
Min.	minute
Ml	milliliter
MMR	measles, mumps, rubella
mg	milligram
min	minute
ml.	milliliter
mo (line over the o)	mother
MPD	Multiple Personality Disorder
MSDS	Material Safety Data Sheets
Mtg	meeting
MSW	Master of Social Work
MVA	Motor Vehicle Agency
N	
NA	not applicable
neg	negative
NKA	no known allergies
Noc	night
NPO	nothing by mouth
Nsg	nursing
N&V	nausea and vomiting
O	
OCD	Obsessive Compulsive Disorder

OD	overdose
OPC	Outpatient Psychiatric Clinic
OP	out-patient
OT	occupational therapy
OTC	over the counter
oz.	ounce
P	
p (with line over p)	after
path.	pathology
p.c./PC	after meals
PCN	penicillin
PEERLA	pupils equal, round and react to light
per	by
PG	pregnant
P.M.	evening
PO	phone order
PRE	progressive resistive exercise
precip.	Precipitating
PRN/p.r.n.	as necessary/whenever necessary
prob.	problem
Psych	psychiatry/psychology
PTP	preliminary treatment plan
PTSD	Post Traumatic Stress Disorder
px.	prognosis
Q	
q	every
QBH	Quality Behavioral Health, Incorporated
q.2h	every two hours
qt.	Quart
R	
R	respirations
re:	about
rec	recreation
resp	respirations
R/O	rule out
ROM	range of motion
RN	Registered Nurse
RTP	return to program
R/T	related to
Rx	treatment, therapy, take (prescription)
S	
secl	seclusion/secluded
sib/SIB	sibling
subcut/subq	subcutaneous
s/e	side effect
S.M.W.D. Sep.	single, married, widowed, divorced, separated
S.O.B.	shortness of breath
S.O.	significant other
S..S.	Social Security
Stat	immediately
STD	Sexually Transmitted Disease
Sx	symptoms
T	

tbsp	tablespoon
ther.	Therapist
trans	transport/transportation
tsp	teaspoon
TB	tuberculosis
Td	tetanus and diphtheria vaccine
TO	telephone order
TPR	temperature, pulse, respirations
Tx	traction/treatment
U	
U	unit
UCG	urine chronic gonadotropin
URI	upper respiratory infection
UTI	urinary tract infection
V	
VD	venereal disease
VO	verbal order
VS	vital signs
W	
w/	with
w/c	wheelchair
wk	week
WNL	within normal limits
w/o	without
wt.	weight
WNL	within normal limits
X	
x	times (as in 4x week)
Y	
Y/O	year old

SYMBOLS

@	at
"	inches
1:1	one to one
#	pound
<	less than, decrease
>	greater than, increase
	female
	male
-	negative
+	positive
	Degree
'	foot
L (circled)	left
R (circled)	right
c (line over lower case c)	with
s (line over lower case s)	without
%	percent

QUALITY BEHAVIORAL HEALTH, INC.

HIPAA APPLICATION AND DATA CRITICALITY ANALYSIS F O R M

Assess the Criticality of the Organization's Applications and Data

Use this form to help you identify the order in which to restore systems after a [illegible] workarounds or alternatives that would allow the organization to continue to use [illegible] form based on input from key department/office representatives and IT staff. Apply criticality decisions to Contingency, Back-up, and Emergency Restoration Plans.

The form asks you to list each application and the data used by that application [Col. 1], describe the function of each application or set of data [Col. 2], and list the IT systems that support the application or set of data [Col. 3]. It then asks you to note [illegible]

APPLICATIONS & DATA CRITICALITY ANALYSIS

Application/Data*	Function	Supporting IT Systems	Consequences of Disruption	Workaround/ Alternative+	Maximum Downtime	Criticality Level**
Lab system/patient test results	*Result reports*	*LAN file server*	*Patient health/safety jeopardized without manual reports*	*Manual reporting*	*72+ hrs.*	*Low*
E-mail/incoming and outgoing messages	*Communication with staff, patients, and* [illegible]	*E-mail server and application*	*More difficult and less timely communications*	*Telephones, faxes, person-to-person*	*50 hrs.*	*Moderate*
Spreadsheet/patient financial information	*Accounts payable*	*LAN file server*	*Delay in billing or payment confirmation*	*Access information directly from* [illegible]	*72+ hrs.*	*Low*

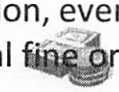
the application or access the data if a disruption occurs [Col. 5]. You then must enter the maximum amount of time the organization could continue to operate without the application and data based on the disruption consequences and workarounds [Col. 6]. Finally, using all of the information on the form, place a relative value on the criticality of your applications and data [Col. 7].

Note that I've filled in examples on the first few lines of the form to help get you started. Remove these on your actual assessment.

*Information system includes: hardware and software, information/data, applications and communication necessary to create, access, transmit and/or store PHI/ePHI.
**What of these is essential/critical information elements needed during an emergency situation?
+In an emergency what roles/responsibilities belong to whom during the emergency AND for the process of full restoration?

HIPAA COMPLIANCE...IT IS SERIOUS BUSINESS!

- ALL consumer information is CONFIDENTIAL, no matter what its form...oral, written, electronic – treat it accordingly. 

- Failure to follow HIPAA confidentiality and security requirements <u>will</u> result in disciplinary action, even termination. Additionally, you may incur a substantial federal fine or imprisonment for purposeful violations.  

- Follow the "minimum necessary" rule when exchanging consumer information with other providers – provide only what is essential to the situation.

- Never leave written or electronic consumer information unattended...lock it, log off it, shut it off are your options.  

- All electronic media with access to confidential information must be password protected...
  - ✓ NEVER SHARE YOUR PASSWORD WITH ANYONE! 
  - ✓ Change your password at least every 90 days.
  - ✓ Make your password complex...combine letters, characters and numbers.
  - ✓ Never write your password down. If you need a reminder, use a phrase or word that means something only to you.

- If it is not web-based, encrypted and password protected it must be backed up and securely stored. The back-up source must be encrypted and password protected too. 

- Anti-virus, malware and firewall protections are a MUST for any media that stores or accesses confidential information. 

- Consumer information disclosures are done ONLY by Medical Records at the Home Office. 

- Use of at work and/or involvement with current or former consumers on any social interaction sight is not ever allowed.

QUALITY BEHAVIORAL HEALTH, INC. MAT BUSINESS ACCESS CONFIDENTIALITY AGREEMENT

CONFIDENTIALITY AGREEMENT

This Agency is required to maintain compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH). These laws protect identify of, and any personal information concerning, any QBH consumers or prospective consumers and their families.

We realize that some persons need to access our facility to accomplish the business activities of the Agency. Therefore, we require all persons who have access to buildings, offices and/or waiting areas to sign this document that testifies that the person signing understands and will comply with the following:

1. Any person that you may recognize while inside or near QBH's buildings will not be acknowledged, nor will you convey to anyone at any time your knowledge that this person has been present at QBH.

2. Should you overhear a name of anyone present at QBH, you will not convey to anyone at any time your knowledge that this person has been present at QBH.

Failure to sign this document and/or failure to abide by its contents may result in legal action and/or a determination that you can no longer access QBH during your business activities.

Your signature will indicate your agreement to maintain compliance with this agreement at any time that you visit/access QBH's facilities.

_____/_____

Signature Printed Name

_____ _____

Position/Job Title Date

Thank you for you cooperation in helping to maintain compliance with these laws.

QBH Management

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement effective on _____ is entered into by and between Business Associate and _____.

Recitals:

A. The purpose of this Agreement is to comply with the Standards for Privacy of Individually identifiable Health Information (Protected Health Information, PHI) published on December 28, 2000, by the Secretary of the U.S. Department of Health and Human Services (HHS) to amend 45 CFR Part 106 and 164 (the Privacy Regulation) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

B. The parties have a prior contract dated _____ (the Service Contract) under which the Business Associate regularly uses and/or disclosures protected health information in its performance of service for _____.

C. This Agreement sets forth the terms and conditions pursuant to which protected health information that is provided by, or created or received by, the Business Associate from or on behalf of _____ will be handled.

Now, therefore, in consideration of the foregoing and of the mutual covenants and agreements hereinafter addressed, the parties agree as follows:

1. Services:

   The Business Associate provides services for _____ that involve the use and disclosure of protected health information which services are described in contract cite. Except as otherwise specified herein, the Business Associate may make any and all uses of protected health information necessary to perform its obligations as set for the in contract cite between the parties. Additionally, the Business Associate may disclose protected health information for the purposes authorized by this Agreement only (a) to its employees, subcontractors and agents, in accordance with Section 2(d), or (b) as directed by _____.

2. Responsibilities of Business Associate:

   With regard to its use and/or disclosure of protected health information only as permitted or required by this Agreement or as otherwise permitted by law:

   a. Use and/or disclose the protected health information only as permitted or required by this Agreement or as otherwise permitted by law;

   b. Report to the designated privacy officer of _____, in writing, any use and/or disclosure of the protected health information that is not permitted or required by this Agreement of which the Business Associate becomes aware

within fifteen (15) days of the Business Associate's discovery of such unauthorized use and/or disclosure;

c. Use commercially reasonable efforts to maintain the security of the protected health information and to prevent unauthorized use and/or disclosure of such protected health information;

d. Require all of its employees, representatives, subcontractors or agents that receive or use or have access to protected health information under this Agreement to agree in writing to adhere to the same restrictions and conditions on the use and/or disclosure of protected health information that apply herein, including the obligation to return or destroy the protected health information as provided under (h) of this section;

e. Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining _____'s compliance with the Privacy Regulation, subject to attorney-consumer or other applicable legal privileges;

f. Upon written request, make available during normal business hours at the Business Associate's offices all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to _____ within ten (10) days for the purposes of enabling _____ to determine the Business Associate's compliance with the terms of this Agreement;

g. Within forty-five (45) days of receiving a written request from _____, provide to _____ such information as is requested by _____ to permit _____ to respond to a request by the subject consumer for amendment and accounting purposes of the disclosures of the consumer's protected health information in accordance with 45 CFR §164.526 and §164.528;

h. Return to _____ or destroy, as requested by _____, within ten (10) days of the rumination of this Agreement, the protected health information in the Business Associate's possession and retain no copies or back-up tapes.

3. Responsibilities of _____:

With regard to the use and/or disclosure of protected health information by the Business Associate, _____ hereby agrees:

a. To inform the Business Associate of any changes in the form of notice of privacy practices that _____ provides to consumers pursuant to 45 CFR §164.520 and provide the Business Associate a copy of the notice currently in use;

b. To inform the Business Associate of any changes in, or withdrawal of, the authorization provided to _____ by consumers whose protected health information may be used or disclosed by the Business Associate under this Agreement pursuant to 45 CFR §164.506 and §164.508; and

c. To notify the Business Associate, in writing and in a timely manner, of any restrictions on the use and/or disclosure of protected health information agreed to by _____ as provided in 45 CFR §164.522.

4. Mutual Representation and Warranty:

Each party represents and warrants to the other party that all of its employees, agents, representatives and consumers of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

5. Terms and Termination:

a. Term: This agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

b. Termination: As provided under 45 CFR §164.504(e)(2)(3)), _____ may immediately terminate this Agreement and any related agreement if it determines that the Business Associate has breached a material provision of the Agreement. Alternatively, _____ may choose to: 1) provide the Business Associate with thirty (30) days written notice of the existence of an alleged material breach; and 2) afford the Business Associate an opportunity to cure said breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of this Agreement. If termination is not feasible, _____ shall report the breach to the Secretary of HHS. This Agreement will automatically terminate without any further action of the parties upon the termination or expiration of the Service Contract.

6. Survival:

The respective rights and obligations of the Business Associate and _____ under the provisions of Section 2(h) and 8 shall survive the termination of this Agreement indefinitely.

7. Amendment:

This Agreement may not be modified or amended, except in writing as agreed to by each party.

8. No Third Party Beneficiaries:

Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

9. Notices:

Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to Business Associate:

If to _____: _____
(Address)

_____ _____
Business Associate, Company Date

_____ _____
Michael Thompson, Executive Director Date

SPECIAL ISSUE – do not use these dangerous abbreviations or dose designations on forms nor in documentation

Abbreviation/Dose Expression	Intended Meaning	Misinterpretation	Correction
Apothecary symbols	dram minim	Misunderstood or misread (symbol for dram misread for "3" and minim misread as "mL").	Use the metric system.
AU	aurio uterque (each ear)	Mistaken for OU (oculo uterque – each eye).	Don't use this abbreviation.
D/C	discharge discontinue	Premature discontinuation of medications when D/C (intended to mean "discharge") has been misinterpreted as "discontinued" when followed by a list of drugs.	Use "discharge" and "discontinue."
Drug names			Use the complete spelling for drug names.
ARA°A	vidarabine	cytarabineARA°C	
AZT	zidovudine (RETROVIR)	azahioprine	
CPZ	COMPAZINE (prochlorperazine)	chlorpromazine	
DPT	DEMEROL-PHENERGAN-THORAZINE	diptheria-pertussis-tetanus (vaccine)	
HCl	hydrochloric acid	potassium chloride (The "H" is misinterpreted as "K.")	
HCT	hydrocortisone	hydrochlorothiazide	
HCTZ	hydrochlorothiazide	hydrocortisone (seen as HCT250mg)	
MgS04	magnesium sulfate	morphine sulfate	
MS04	morphine sulfate	magnesium sulfate	
MTX	methotrexate	mitoxantrone	
TAC	triamcinolone	tetracaine, ADRENALIN, cocaine	
ZnS04	zinc sulfate	morphine sulfate	
Stemmed names			
"Nitro" drip	nitroglycerin infusion	sodium nitroprusside infusion	
"Norflox"	norfloxacin	NORFLEX	
ug	microgram	Mistaken for "mg" when handwritten.	Use "mcg."

o.d. or OD	once daily	Misinterpreted as "right eye" (OD – oculus dexter) and administration of oral medications in the eye.	Use "daily."
TIW or tiw	three times a week	Mistaken as "three times a day."	Don't use this abbreviation.
per os	orally	The "os" can be mistaken for "left eye."	Use "PO," "by mouth," or "orally."
q.d. or QD	every day	Mistaken as q.i.d., especially if the period after the "q" or the tail of the "q" is misunderstood as an "i".	Use "daily" or "every day."
qn	nightly or at bedtime	Misinterpreted as "qh" (every hour).	Use "nightly."
qhs	nightly at bedtime	Misread as every hour.	Use "nightly."
q6PM, etc.	every evening at 6 PM	Misread as every six hours.	Use 6PM "nightly."
q.o.d. or QOD	every other day	Misinterpreted as "q.d." (daily) or "q.i.d. (four times daily) if the "o" is poorly written.	Use "every other day."
sub q	subcutaneous	The "q" has been mistaken for "every" (e.g., one heparin dose ordered "sub q 2 hours before surgery" misunderstood as every 2 hours before surgery).	Use "subcut" or write "subcutaneous."
SC	subcutaneous	Mistaken for SL (sublingual).	Use "subcut" or write "subcutaneous."
U or u	unit	Read as a zero (0) or a four (4), causing a 10Ƴfold overdose or greater (4U seen as "40" or 4u seen as 44").	"Unit" has no acceptable abbreviation. Use "unit."
IU	international unit	Misread as IV (intravenous).	Use "units."
cc	cubic centimeters	Misread as "U" (units).	Use "mL."
x3d	for three days	Mistaken for "three doses."	Use "for three days."
BT	bedtime	Mistaken as "BID" (twice daily).	Use "hs."
ss	sliding scale (insulin) or ½ (apothecary)	Mistaken for "55."	Spell our "sliding scale." Use "one-half" or use "1/2."

< and >	less than and greater than	Mistakenly used opposite of intended.	Use "greater than" or "less than."
/ (slash mark)	separates two doses or indicates "per"	Misunderstood as the number 1 ("25 unit/10 units" read as "110" units.	Do not use a slash mark to separate doses. Use "per."
Name letters and dose numbers run together (e.g., Inderal40mg)	Inderal 40 mg	Misread as Inderal 140 mg.	Always use space between drug name, dose and unit of measure.
Zero after decimal point (1.0)	1 mg	Misread as 10 mg if the decimal point is not seen.	Do not use terminal zeros for doses expressed in whole numbers.
No zero before decimal dose (.5mg)	0.5 mg	Misread as 5 mg.	Always use zero before a decimal when the dose is less than a whole unit.

ELECTRONIC MEDIA MAINTENANCE LOG

Office/Department: ______________________________ **Year:** ____________

NAME OF MAINTENANCE ORGANIZATION/ CONTRACT	FUNCTION A=Administrative C=Clinical staff T=IT personnel M=Maintenance O=other ______	ACCESS TO: (Check all that apply)			COMMENTS (e.g. dates present; all/most work day access; 7 day/wk. access) or other pertinent info
		FACILITY	INTERNET	PHI/ePHI	

ELECTRONIC MEDIA MOVEMENT LOG

Computer ID #	Date of Transfer	Who Received	Date returned	Reason for Transfer

COMPLAINT/BREACH INVESTIGATION REPORT

NATURE OF BREACH: ___ Written Complaint ___ Suspected breach ___ Known breach

If complaint, was DHHS and/or JC notified by complainant? ___ No ___ Yes
Date entered in HIPAA Complaints/Violations Log: _____

THOSE WHO CAUSED/CONTRIBUTED TO THE BREACH

___ Staff _____ _____
(NAME/POSITION) (NAME/POSITION)

___Consumer/Guardian _____
(NAME)

___ Business Associate _____
(NAME)

___ Imposter _____
(NAME OR DESCRIPTION, IF KNOWN)

DEMOGRAPHICS

Location of breach: _____

Date of breach, if ascertainable: _____

Date breach identified: _____

Date/time Security/Privacy Officer notified: _____/_____ AM/PM

Date/time CEO notified: _____/ _____ AM/PM

Initially reported by:

___ Person who created the breach _____
(NAME)

___ Person who discovered the breach _____

QUALITY BEHAVIORAL HEALTH, INC. MAT COMPLAINT/BREECH INVESTIGATION REPORT

(NAME)

___ Another person _____

(NAME)

Describe how they knew of the breach: _____

FINDINGS OF INVESTIGATION

Nature of the violation and whether person(s) accessing the information would know what it was or what they could do with it:

Did exposure of information occur and, if so, how it has been used or disbursed, if known:

Number of consumers/families affected:

Time period during which the violation occurred:

Nature and extent of harm resulting, including physical harm, financial harm, harm to a consumer's reputation, hindrance to consumer's ability to obtain health care:

QUALITY BEHAVIORAL HEALTH, INC. MAT COMPLAINT/BREECH INVESTIGATION REPORT

Describe if any harm has already occurred at the time of or prior to the investigation:

Nature of any mitigation activities that have or are now being initiated:

If notice outside the Organization is indicated, identify who (consumers/guardians, media, law enforcement, HHS*) will be noticed, how and date: *Must report immediately if 500+ consumers were exposed OR within 60 days after the end of the calendar year provide notice on the HHS website if less than 500 consumers involved.

History of prior noncompliance by violator:

Whether attempt was made to correct any noncompliance by the violator:

Response of violator to prior complaints/investigations, if applicable:

QUALITY BEHAVIORAL HEALTH, INC. MAT COMPLAINT/BREECH INVESTIGATION REPORT

Any other factors/circumstances/findings realized during the investigation:

INTERNAL CONCLUSION RE BREACH

___ Violation(s) where violator did not know or would not have known of the breach

___ Violation(s) with reasonable cause without willful neglect /intent

___ Violation(s) with willful neglect /purposeful intent

DETERMINATION AFTER INVESTIGATION:

___ Unintentional initial violation
___ Unintentional; repeat of prior violation(s)
___ Intentional

ACTIONS TAKEN UPON RECEIPT OF COMPLAINT/REPORT OF VIOLATION AND INITIAL INVESTIGATION

By Security or Privacy Officer:

___ Verbal reprimand and immediate retraining related to area of violation

___ Written warning and training documentation to HR file Date: _____

___ Directive for formal retraining in HIPAA/HITECH Security and Confidentiality Policies within 2 weeks.

___ Notice to HR Manager/Clinical Director for training Date: _____

___ After consultation with CEO, instructed to not return to work till further notice after Clinical Committee has convened and to remain available for interview

___ Other action: _____

By Clinical Committee (and/or CEO): Date of decision: _____

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

HIPAA PRIVACY INSPECTION CHECKLIST
(Consumer is used to refer to both consumer and staff information that is considered private under privacy laws.)

OFFICE/DEPT: _____ **DATE:** _____

INSPECTION ITEMS	FINDINGS/COMMENTS
AUDITORY PRIVACY	
Consumer related discussions conducted beyond consumer/visitor hearing	
Consumer information shared verbally with only those "in need to know"	
Only consumers' first names used in front office/waiting area to call up a consumer	
Phone conversation with/ related to a consumer cannot be overheard by others	
Voice messages are listened to at a low volume and away from the hearing of others if possible	
VISUAL PRIVACY	
Consumer information cannot be viewed at the reception area	
Computers have security screens and/or are kept positioned away from view of general public	
Consumer sign in uses method so that the consumer's sign in can be removed or blocked from view as soon as they have signed in, or uses first name only	
Consumer information is not visible on staff desks/work areas when unattended by staff member	

Consumer information is not posted where non-staff persons can view it	
Fax transmissions have a confidentiality statement included	
Mail, both incoming and outgoing, is kept away from public view	
Interoffice mail is sent in approved envelopes and marked confidential; interoffice mail area is not in public view	
Information to be shredded is shredded promptly or stored in a secured container till shredded	
Staffs' children and spouses do not accompany or visit inside offices	
SECURITY OF CONSUMER INFORMATION	
Consumer information is not left unsecured during absences of staff from their offices	
Confidential records work/ storage areas are not left unattended/unsecured (e.g. fax machine, copier)	
Confidential records work/ storage areas are restricted to only those with "need to know" access (e.g. fax machine, copier)	
All confidential records are kept secured when not in the presence of the staff who signed them out	
Confidential records are not found in "unauthorized" areas	
Faxed consumer information has a confidentiality disclosure statement on the cover sheet	

Consumer information is not distributed in any hard copy format without a consumer release of information authorization	
Release of information authorizations are filled out completely and correctly • What info can be released • To whom it may be released • Timeframe consent is for • Signed by consumer/ guardian	
Consumer information shared verbally is only shared with those that, by HIPAA law, have a "right to know"	
Every consumer receives a current Notice of Privacy Practices document at admission	
"Business associates" sign a confidentiality agreement prior to access to clinical records (Check with HR)	
Medical Records keeps a log of all releases of consumer information/reviews of the consumer record (whether hard copy or electronic) by authorized persons	
Electronic records are not left open when the user is away from the area and/or if someone unauthorized to see the record enters the area	
SECURE TRANSPORT	
All hard copy consumer information is transported from one location to	

another in a locked container	
Vehicular transport of consumer information is inside a locked container and in a locked trunk or glove box (if neither available – in a location where the likelihood of being tossed from the vehicle is minimal)	
Consumer information is never left at an unauthorized site	
If consumer information is left at a worksite other than the agency (e.g. school office), it is kept in a locked cabinet/drawer within a locked room whenever unattended by clinical staff	
Contingency plan exists for security of paper format confidential records during a disaster – plan is tested at least annually	
Emergency Mode of Operations plan exists for all hard copy confidential records needed to perform business operations – plan is tested at least annually	
KNOWLEDGE OF REQUIREMENTS	
Interview of staff confirms they are knowledgeable or HIPAA and confidentiality practices of the agency	
Staff is educated at least annually and at initial orientation regarding HIPAA and privacy/confidentiality practices of the Company	
Interview of consumers/ guardians confirms they are	

knowledgeable of their rights under HIPAA		
Interview of consumers/ guardians confirms they understand the Notice of Privacy Practices they received at admission		
Staff can state who the Privacy and Security Officers are and how/when they are to be reached		
TOTAL = 39	# COMPLIANT =	PERCENTAGE *=

*Divide # compliant by 39 for percentage. Provide percentage to QM Coordinator after each inspection.

QUALITY BEHAVIORAL HEALTH, INC. MAT **HIPAA PRIVACY INSPECTION CHECKLIST**

PRIVACY INSPECTION FINDINGS REPORT

==========

THIS SECTION TO BE COMPLETED BY PRIVACY OFFICER

DATE OF SURVEILLANCE: _____ INSPECTOR: _____

DEPARTMENT: _____ REPORT RECIPIENT: _____

The following items related to HIPAA and Privacy/Confidentiality Practices were identified to need improvement:

1.
2.
3.
4.
5.

Please inform the Privacy Officer of corrective actions taken within 2 weeks of receiving this report. Thank you for your cooperation.

==========

THIS SECTION TO BE COMPLETED BY MANAGER/DEPARTMENT DIRECTOR OR DESIGNEE

	ACTION TAKEN	DATE RESOLVED
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

SENT TO _____ ON: _____ BY: _____

==========

THIS SECTION TO BE COMPLETED BY PRIVACY OFFICER

RECEIVED BY PRIVACY OFFICER ON: _____

CORRECTIONS: ___ SATISFACTORY ___UNSATISFACTORY

ACTION TAKEN: _____

_____

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

HIPAA PRIVACY REPORT

QUARTERLY REPORT

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
INSPECTION/ENFORCEMENT				
VISUAL PRIVACY				
• Screen positioning				
• Blank/screen saver setting				
• Protection programs				
SECURITY OF PHI				
• No documents/media with PHI/ePHI located where in view or access of consumers/ visitors/staff without need to know				
• Storage sources for PHI are locked when not being attended by authorized staff				
• Electronic media is not left unattended and/or				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
open to access when the staff using it is not within view of it				
• Security/Privacy posters are apparent in workstations				
• Release of Info before any distribution/log of distribution kept by MR				
• No discussions containing PHI occur within hearing of other consumers/visitors/staff without need to know				
• Closure of documents and/or media with PHI when leave or unauthorized person enters area				
• Never leave media unattended/keep locked up (room locked) if not in use				
• Restricted access to workstations				
• Privacy and Security Plans are enforced				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
• Minimum necessary data rule followed				
• Disposal policy followed				
• Maintenance/repair log maintained				
SECURE TRANSPORT				
• Never left at unauthorized site				
• Locked up when unattended within a locked room				
KNOWLEDGE OF:				
• Confidentiality practices				
• Penalties for violations				
• Name of Privacy and Deputy Privacy Officers (if applicable)				
• Prompt reporting of breaches/security incidents				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
• HHS visit to sites Disaster recovery plan/ emergency mode operations plan – their role for hard copy and removable media containing PHI/ePHI				
HIPAA SYSTEM EVALUATIONS (Jointly with Security Officer et al)				
RISK ANALYSIS • Annual				
APPLICATIONS AND DATA CRITICALITY ANALYSIS • Annual				
REVIEW OF RECORDS/REPORTS • Quarterly • All HIPAA related logs/reports related to Privacy processes				
CONTINGENCY PLAN TESTING [Credible and other electronic programs/documents]				
EMERGENCY MODE OPERATION PLAN • Annual				
DISASTER RECOVERY PLAN • Annual				
HIPAA SYSTEM EVENTS [AS THEY OCCUR]				
OFFICER APPOINTMENTS				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
OFFICER/DEPUTY TRAINING • Annual • As needed				
STAFF TRAINING • Annual • As needed				
HIPAA GUIDELINES • Policy review – annual • State changes – annual • Federal changes - annual				
BREACHES/COMPLAINTS				
BREACHES				
• Identified or reported in report period/for year o Intentional o Unintentional				
• Status of investigation Results of investigation				
COMPLAINTS				
• Received in report period/for year				

Initiated: 2/2022
Reviewed/Revised:2/2023, 1/2024, 1/2025

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
• Status of investigation				
• Results of investigation				
• Investigation Report attached for each				
MISCELANEOUS				

Note: With findings, remember that trended information (bar graph, pie chart or similar tool) should be attached to reflect trends or patterns.

Instructions:

1. Provide aggregate (may also break out by location) findings (positive or negative) from HIPAA Security Activities in "Findings" column. If no negative findings for an activity, report "all in compliance" in that activity's "Findings" box.
2. When recommendations or actions have been or need to be taken, indicate: whether the recommendation or action is "P" which means it is a preventive measure being taken to avoid a problem/issue, not a response to a problem/issue identified; or whether it is "R" which means the recommendation or action is in response to a problem/issue that has already occurred.
3. Describe the recommendation being made or the action already taken or to be taken, include the date by which it should be or was done, if feasible.
4. If/when a recommendation is carried out and/or an action is completed indicate what the status of the intervention is or, if already completed, what degree of effectiveness/improvement was achieved. This means that items from previous reports may carry over to the next until any problems/issues are reported as fully resolved.

HIPAA SECURITY REPORT

QUARTERLY REPORT

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
INSPECTION/ENFORCEMENT				
VISUAL PRIVACY				
• Screen positioning				
• Blank/screen saver setting				
• Protection programs				
SECURITY OF ePHI				
• No consumer identifiers in non-encrypted/non password protected media				
• Electronic media w/ PHI encrypted				
• No PHI on personal electronic media				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
• Security posters				
• Release of Info before any distribution/log of distribution kept				
• Audit, access and security incident logs maintained				
• Access termination followed				
• Closure of media when leave or unauthorized person enters area				
• Never leave media unattended/keep locked up if not in use				
• Restricted access to workstations				
• Password assignment w/ profile code				
• No shared passwords				
• Password changes – 90 days				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
• Encrypted/password protected data back up				
• Movement accountability record maintained				
• Security Plan enforced				
• Minimum necessary data rule followed				
• Disposal policy followed				
• Maintenance/repair log maintained				
SECURE TRANSPORT				
• Never left at unauthorized site				
• Locked up when unattended within a locked room				
KNOWLEDGE OF:				
• Confidentiality practices				
• Penalties for violations				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
• Name of Security and Deputy Security Officers				
• Prompt reporting of breaches				
• HHS visit to sites				
• Business Associate agreement required – leaders only				
• Disaster recovery plan/emergency mode operations plan				
HIPAA SYSTEM EVALUATIONS				
RISK ANALYSIS • Annual				
APPLICATIONS AND DATA CRITICALITY ANALYSIS • Annual				
REVIEW OF RECORDS/REPORTS • Quarterly • All HIPAA related logs/reports				
CONTINGENCY PLAN TESTING [Credible and other electronic programs/documents]				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
DATA BACK UP PLAN • Annual at each office				
EMERGENCY MODE OPERATION PLAN • Annual				
DISASTER RECOVERY PLAN • Annual				
HIPAA SYSTEM EVENTS [AS THEY OCCUR]				
OFFICER APPOINTMENTS				
OFFICER/DEPUTY TRAINING • Annual • As needed				
STAFF TRAINING • Annual • As needed				
EMR and other ELECTRONIC SYSTEMS • Changes • Additions				
HIPAA GUIDELINES • Policy review – annual • State changes – annual • Federal changes - annual				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS
BREACHES/COMPLAINTS				
COMPLAINTS				
• Received in report period/for year				
• Status of investigation				
• Results of investigation				
BREACHES				
• Identified or reported in report period/for year o Intentional o Unintentional				
• Status of investigation				
• Results of investigation				
• Investigation Report attached for each				
MISCELANEOUS				
HIPAA VISIT				

ACTIVITY	FINDINGS	PROACTIVE = P RESPONSIVE = R	RECOMMENDATIONS/ACTIONS AFTER ANALYSIS	STATUS OR RESULTS/EFFECTIVENESS

Note: With findings, remember that trended information (bar graph, pie chart or similar tool) should be attached to reflect trends or patterns.

Instructions:

1. Provide aggregate (may also break out by location) findings (positive or negative) from HIPAA Security Activities in "Findings" column. If no negative findings for an activity, report "all in compliance" in that activity's "Findings" box.
2. When recommendations or actions have been or need to be taken, indicate: whether the recommendation or action is "P" which means it is a preventive measure being taken to avoid a problem/issue, not a response to a problem/issue identified; or whether it is "R" which means the recommendation or action is in response to a problem/issue that has already occurred.
3. Describe the recommendation being made or the action already taken or to be taken, include the date by which it should be or was done, if feasible.
4. If/when a recommendation is carried out and/or an action is completed indicate what the status of the intervention is or, if already completed, what degree of effectiveness/improvement was achieved. This means that items from previous reports may carry over to the next until any problems/issues are reported as fully resolved.

QUALITY BEHAVIORAL HEALTH, INC. MAT INVENTORY OF PHYSICAL SYSTEMS DEVICES AND MEDIA LOG

INVENTORY OF PHYSICAL SYSTEMS DEVICES AND MEDIA LOG

OFFICE/DEPT.	PHYSICAL SYSTEM Device/Media Identifier	ePHI USE: (Check all that apply)				COMMENTS
		STORE	ACCESS	CREATE	TRANSMIT	

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

QUALITY BEHAVIORAL HEALTH, INC. MEDICAL RECORD CHECKLIST

Date File was checked Date File was checked again Date File was checked again

ORIENTATION	RESPONSIBILITY	DEADLINE	COMMENTS Accurate/timely/complete	SIGNATURE
	Intake	Upon Admission		
Consumer's referral Form (ALL CONSUMERS)	Intake	Upon Admission		
Picture ID (ALL CONSUMERS)	Intake	Upon Admission		
SSN (ALL CONSUMERS)	Intake	Upon Admission		
Medicaid Card (ALL MEDICAID CONSUMERS)	Intake	Upon Admission		
Unit/Service Orientation (ALL CONSUMERS)	Unit staff/Outpatient Intake	Arrival to unit/ Upon Admit to OP		
CONSENT	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Consent to Treatment (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Medication Notification Agreement (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Recipient Rights Acknowledge Form (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Medicaid Recipient Complaint/ Grievance Rights Process (MEDICAID CONSUMERS)	Intake/ Consumer	Upon Admission		
Administrative Tribunal (MEDICAID CONSUMERS)	Intake/ Consumer	Upon Admission		
Authorization to Request/ Release Information (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Consumer Notice of Confidentiality (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Rules and Regulations (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Consumer Fee Agreement (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
No Pass Contract (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
Important Consumer Information Form (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
HIPAA (ALL CONSUMERS)	Intake/ Consumer	Upon Admission		
ASSESSMENT	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Assessment Part 1 (ALL CONSUMERS) *Complete and Timely*	Consumer	Upon Admission		
Assessment Part 2 (ALL CONSUMERS) *Complete and Timely*	Nurse	Upon Admission		
Assessment Part 3 (ALL CONSUMERS) *Complete and Timely*	Counselor	Within 24 hrs		
Master Needs List	Counselor	Within 48 hrs		
Clinical Summary of Findings (ALL CONSUMERS)	Counselor	Within 24 hrs		
TREATMENT PLAN	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Individual Treatment Plan (ALL	Counselor	Within 24 hrs		

QUALITY BEHAVIORAL HEALTH, INC. MEDICAL RECORD CHECKLIST

Group Note Response (RESIDENTIAL CONSUMERS)	Counselor/ Consumer	On Going		
Services Billed Match Services Provided (ALL CONSUMERS)	Clinical Staff/ Monitors/Nurses	On Going		
CONSUMER ACTIVITY	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
NURSING	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
PSYCHIATRY	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Medical History and Physical Examination (ALL CONSUMERS) *Complete and Timely*	Dr Hafeez	Within 2 days		
LABORATORY	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
MEDICATIONS	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Prescription (ONLY CONSUMERS WITH SCRIPT)	Nurse	On Going		
CASE MANAGEMENT	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Case Management (ALL CONSUMERS)	Case Managers	Within 10 days		
DISCHARGE AND FOLLOWUP	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
Discharge/ Transfer Letter – 2 Copies (ALL CONSUMERS)	Monitors	When Discharging		
Discharge Summary (ALL CONSUMERS)	Counselor	Within 10 days		
MISC LIST	**RESPONSIBILITY**	**DEADLINE**	**COMMENTS**	**SIGNATURE**
List of Patient's Belongings (ALL CONSUMERS)	Monitors	Upon Admission		
Security Clearance Certificate	Monitors	Admission-reentry		

MEDICAL RECORD PEER REVIEW NURSING FORM QUALITY, ACCURACY, AND COMPLETENESS *LEGEND: Y = YES N = NO NA = NOT APPLICABLE*	
MEDICAL RECORD #	
RECORDER INITIALS	

ASSESSMENT		
INTAKE AND NURSING ASSESSMENTS THOROUGH		
ITEM	**CODE**	**COMMENTS**
a. HEALTH SCREEN DESCRIBES CURRENT AND CHRONIC MEDICAL/MENTAL HEALTH CONDITIONS		
b. BODY SYSTEMS REVIEW		
c. MEDICATIONS HISTORY/USE		
d. NUTRITION SCREEN AND NUTRITION ASSESSMENT IF INDICATED		
e1. PAIN SCREEN		
e2. PAIN ASSESSMENT		
f. COMMUNICABLE DISEASE RISKS		
g. MENTAL STATUS EXAM		
h. VITAL SIGNS		
i. CLINICAL DETERMINATION OF MEDICAL APPROPRIATENESS FOR TREATMENT LEVEL		
j. SCREEN FOR TRAUMA, ABUSE, NEGLECT, AND EXPLOITATION COMPLETE AND ASSESSMENT (if applicable) COMPLETE		

MEDICAL RECORD PEER REVIEW
NURSING FORM
QUALITY, ACCURACY, AND COMPLETENESS

LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #	
RECORDER INITIALS	

ITEM	CODE	COMMENTS
k. CENTRAL REGISTRY VERIFICATION DOCUMENTED (unless done by Counselor or MD.)		
TREATMENT PLANNING		
a. PLAN ADDRESSES CONSUMER'S MEDICAL/NURSING NEEDS AND PREFERENCES		
b. NURSING/MEDICAL TREATMENT IS APPROPRIATE TO LEVEL OF CARE		
c. NURSING TREATMENT IS REVISED AS NEEDS CHANGE AND WHEN INDICATED		
PROGRESS NOTES		
a. NOTES REFLECT NURSING OBSERVATIONS AND RESULTS OFNURSING/MEDICAL THERAPIES		
b. NOTES REFLECT NURSING SERVICES PROVIDED AS IN TREATMENT PLAN/ORDERS		
c. REFLECT SERVICE APPROPRIATE TO THE CONSUMER'S LEVEL OF CARE		
d. SERVICE PROVIDED RELATES TO CONSUMER'S TREATMENT GOALS AND OBJECTIVES		

MEDICAL RECORD PEER REVIEW NURSING FORM QUALITY, ACCURACY, AND COMPLETENESS *LEGEND: Y = YES N = NO NA = NOT APPLICABLE*		
MEDICAL RECORD #		
RECORDER INITIALS		
e. REPORTS OF DIAGNOSTIC AND THERAPEUTIC PROCEDURES WITH ACTION, WHEN INDICATED		
MAR COMPLETED CORRECTLY AND CURRENT		
MED RECONCILIATION DONE AND CURRENT		
MEDICATION EDUCATION DOCUMENTED		
CONCLUSION AT TERMINATION OF CARE/SERVICES		
MEDICAL/NURSING DISCHARGE INSTRUCTIONS TO CONSUMER AND FAMILY		

NOTE: The Quality and Utilization Manager will randomly select at least 3 records for each practitioner for review by another like-type practitioner during each quarter, using the peer review form appropriate to that discipline. Completed reviews are to be submitted to the Quality and Utilization Manager by the deadline communicated when the reviewer was notified which records to review and for which practitioner.

PROCESS	QUESTIONS TO GUIDE ANALYSIS	COMMENTS and ADDITIONAL FACTORS/CONCERNS
Sanctions Process	Have you developed a written sanctions policy against workforce members who do not abide by your policies?	
	Have you explained those sanctions to your workforce members?	
	Do you consistently enforce those sanctions?	
Security Measures Enforcement (Risk Management)	Do you control the information contained on your information system?	
	Do you or your workforce take home portable computers or other devices containing ePHI?	
	Does any vendor have access to confidential consumer data? Have you discussed HIPAA Security and HITECH requirements with such vendor(s)? Is an up-to-date Business Associate Agreement in place for each vendor that has access to ePHI?	
	Can a vendor change confidential consumer data? If so, are you monitoring audit logs for such changes?	
	Do you update your workforce members' training each time you develop and implement new policies and procedures? Do you document initial and continuing training in their HR files?	
	Have you set user access to ePHI? Does access correspond to job descriptions (ex., clinical, administrative, or billing)?	

	Do you monitor reports that identify persons and systems that access ePHI, including those not authorized to have access to ePHI?	
	Do you have control over who can amend your consumer records?	
Review System Activity Regularly	Do you regularly review HIPAA required logs and reports for any issues, trends or patterns, vulnerability issues?	
	Do you regularly review system audit trails that identify who has accessed the system and track additions, deletions, or changes they may have made to ePHI?	
	Would you know if someone was trying to hack into your system? (Do you regularly review security incident reports?)	
	Do you keep an updated inventory of hardware and software owned by each office?	
	Can you identify where ePHI is located (e.g., desktops, laptops, handhelds, tablets, removable media, servers, etc.)?	
	Could you locate the inventory in a disaster (fire, flood, explosion, theft)?	
	Do you know the current approximate value of your hardware and software?	
	Does the inventory contain all necessary contact information, including information for workforce members and service providers?	

Assigned Security and Privacy Responsibilities	Are the job descriptions for these positions current? Are the responsibilities being effectively carried out by the Officers?	
	Have you appointed a Security Official?	
	Do your Privacy and Security Officials coordinate privacy and security policies and procedures? (Privacy and Security Official may be the same person.)	
	Do your Deputies coordinate privacy and security issues with their respective Officers?	
Workforce Security: Authorization/ Supervision/Access	Do you have written job descriptions that define appropriate access to ePHI?	
	Could an unauthorized workforce member obtain access to ePHI?	
	Are persons with access to ePHI supervised?	
Workforce Security: Workforce Clearance Procedure	Do you contact references before hiring employees or contracting for staff?	
	Do you conduct background checks?	
Workforce Security: Termination Procedures	Do you immediately deactivate a workforce member's access upon termination (or, as appropriate, upon change of job description)?	
	Do you notify your IS vendor of a staff's termination within a specific time?	
	Is there a standard checklist of action items when a staff leaves? (Return keys, close and payment of credit cards, return software and hardware)	

	Do you consistently enforce checklists and policies with respect to all staff that are terminated or whose duties have changed, whether the termination or change was voluntary or for cause?	
Info Access Management: Access Authorization	Are you using your IT system's log-in process to authorize access (such as limiting administrative access)?	
	Is each workforce member's access to ePHI based on his or her job description?	
Info Access Management: Access Establishment and Modification	Do you document, periodically review, and modify as appropriate workforce members' access to ePHI?	
Security Awareness: Training	Have you implemented a security awareness and training program for all members of your workforce, including management?	
	Have there been lapses in privacy safeguards that indicate a need for training refreshers?	
	Have you identified your security training priorities?	
Security Awareness: Reminders	Are security reminders posted in a visible location?	
	Are vendors aware of your security reminders?	
	Do workforce members know where to find a copy of your security policies and procedures?	

	Do workforce members understand the consequences of noncompliance with those policies?	
	Are workforce members with laptops, PDAs, or cell phones aware of encryption requirements?	
	Do you consistently follow your security awareness and training program with all new hires?	
Security Awareness: Protection from Malicious Software	Have you installed anti-virus and other anti-malware protection software on your computers? Do you use it to guard against, detect, and report any malicious software? Do you protect against spyware?	
	Do workforce members update the virus protection software when it is routed to them?	
	Do you prohibit workforce members from downloading software they brought in from elsewhere? (Digital family photos, games, books, music, etc.)	
Security Awareness: Log-in Monitoring	Does the Security Officer or Deputy regularly monitor audit logs?	
	Is the Security Officer notified of unsuccessful log-ins?	
	Do workforce members know what to do if they cannot access the system?	
Security Management:	Have you established procedures for creating, changing, and safeguarding passwords?	

Password Management	Are sanctions in place if workforce members share passwords?	
	Do workforce members know what to do if they forget a password?	
	Are you providing password management reminders? Are changes occurring every 90 days?	
Security Incidents/Breaches: Response and Reporting	Do you know if your security system has ever been breached?	
	Have you prioritized what must be restored in the event of a system disruption?	
	Have you developed a list of persons and entities to contact in the event of a security incident?	
	Do you require workforce members to tell you immediately if they suspect a compromise to your system?	
	Have you made a list of possible security incidents?	
	Do you document all security incidents and their outcomes?	
Contingency Planning: Data Backup	Does each office back up its electronic data?	
	Do you store the backup data at the office location (unless web based)?	
	Do you know whom to call to restore data?	
Contingency Planning: Disaster Recovery	Do you have a procedure to restore any loss of data?	
	Do you have a list of critical hardware, software, and workforce members?	

Contingency Planning: Emergency Mode Operation Plan	If you are required to operate in emergency mode, do you have procedures to enable you to continue critical business processes to protect the security of ePHI?	
	Do you have a plan to temporarily relocate if you lose access to your physical location?	
	Would ePHI be safeguarded in this temporary location?	
	Are formal agreements in place for such a re-location?	
	Have you trained staff on your contingency plan?	
	Is there a contingency plan coordinator?	
	Do you have an emergency call list?	
	Have you identified situations in which your contingency plan must be activated?	
	Is there a plan to restore systems to your normal operations?	
Contingency Planning: Testing and Revision Procedures	Have you tested your contingency plan? At the frequency established? Have glitches been addressed?	
Contingency Planning: Applications and Data Criticality Analysis	Do you have a plan to restore your business activities, beginning with what is most critical to your practice?	
Business Associate Contract	Are all necessary Business Associate Agreements in place? Are they HIPAA and HITECH compliant?	
	Are there new organizations or IT vendors that require a Business Associate Agreement?	

	Is the BA log current?	
Inspection/Evaluation	Do you perform periodic HIPAA Security inspections/evaluations? Are they done at least quarterly?	
	Do you also perform these evaluations in response to environmental and operations changes affecting the security of your ePHI, to determine whether your security policies and procedures meet HIPAA Security requirements?	
	Do you perform both technical and nontechnical evaluations?	
	Has your Security Officer determined acceptable levels of risk in its business operations and mitigation strategies?	
	Do you have a plan to evaluate your systems at least annually, and at any time a risk warrants a review?	
Facility-Specific Security Safeguards	Do you know who needs access to the facility in the event of a disaster?	
	Do you have a backup plan for access, including who has authority to access the facility in a disaster?	
	Do you have an inventory of facilities and equipment therein?	
	How do you safeguard your facility and equipment from unauthorized physical access, tampering, and theft?	
	Is there a contingency plan in place and known by each office?	

	Do you have procedures in place to control physical access to your facility and areas within your facility where PHI/ePHI could be accessed?	
	Do you validate a person's authority to access software programs for testing and revision?	
	Is there a history or risk of break-ins that requires monitoring equipment?	
	If monitoring or surveillance equipment generates records or footage, how is it reviewed, handled, and disposed of?	
	If you use a security contractor for surveillance purposes, do you have an up-to-date Business Associate Agreement in place with the contractor?	
Maintenance Records or Log	Have you repaired or modified any physical components at any offices related to security, such as doors, locks, walls, or hardware, or do you expect to do so?	
	Do you have a system to document all such repairs and modifications?	
Workstation Use/Security	Have you documented how workstations are to be used in each office?	
	Are there wireless tools used as workstations?	
	Can unauthorized persons view content of workstations?	
	Is access to ePHI restricted to authorized users? Is it enforced?	

	Is there a log-off policy before leaving computers unattended? Is it consistently employed?	
	Is there a policy that controls Internet access while working with ePHI?	
Device/Media Controls: Disposal	Do you destroy data on hard drives and file servers before disposing the hardware?	
Device/Media Controls: Media Re-use	Are workforce members trained as to the security risks of re-using hardware and software that contain ePHI?	
	Do you have a procedure for removing ePHI from electronic media before it can be re-used?	
Device/Media Controls: Movement Accountability Log	Do you document the movement of hardware and electronic media and who is responsible for each item?	
	Do you periodically check the inventory to ensure computers are where they are supposed to be?	
	Do you document where they've been moved?	
	Is the inventory list part of your disaster recovery files? Is it stored in a disaster-proof manner, i.e., offsite and (preferably) electronically?	
Device/Media Controls: Data Backup and Storage	Do you regularly back up data on hardware and software and maintain backup files off site or to a web-based location?	
	Do you back up ePHI before equipment is moved?	

	Have staff members been trained on backup policies?	
Access Control: Unique User Identification	Has the Security Officer or designee assigned a unique user identity to each member of the workforce?	
	Are passwords unique to each individual and not shared?	
	Is there a sanction policy on sharing passwords?	
	Do workforce members have access to the minimum ePHI necessary to perform their job responsibilities?	
	Do you participate in ePrescribing or comparable electronic medication ordering? If so, does the system validate your electronic signature? Are physicians the only providers allowed to ePrescribe et al in your Organization?	
Access Control: Emergency Access Procedure	Does the Security Official have a unique user ID that is used only in emergencies?	
	Is there a process to notify another leader in the practice when the emergency ID is used?	
Access Control: Automatic Logoff	Do your computers/other media automatically log off after a specific period of inactivity?	
	Is there a shorter log off period for computers/other media in high traffic areas?	
	Do you send e-mail containing ePHI to consumers?	

Access Control: Encryption and Decryption	Is the e-mail sent over an open network such as AOL, Yahoo, Gmail, EarthLink, or Comcast?	
	Do you have a mechanism in place to encrypt and decrypt ePHI?	
Audit Controls	Is there a procedure in place to monitor and audit workforce members with access to ePHI and their activity with respect to ePHI?	
	Is one person responsible for conducting audit processes and reporting results?	
	Has your IT/EMR vendor explained how to conduct audits?	
Audit Controls: Mechanism to Authenticate ePHI	Are users required to authenticate themselves when logging on to the system?	
	Is there a feature that locks out users after a specific number of failed log-in attempts?	
	Does the system allow you to conduct audit trails on users?	
Integrity Controls	Have you identified sources that would jeopardize the integrity of ePHI (vandalism, hackers, system failures, viruses)?	
	Is there an electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?	
	Does the software allow you to track and audit users who transmit and alter ePHI?	
Person or Entity Authentication	Does your system require users to identify themselves using a password and user name?	

Transmission Security	Is data transmitted through standard network protocols?	
	Does the IT/EMR vendor ensure that information is not altered in transmission?	
	Is there an auditing process in place?	
	Does your Organization use a mechanism (secure network) to encrypt e-mail or other ePHI?	
	Does your Organization send ePHI via handhelds or wireless laptops?	
	Do workforce members know how to respond to e-mails containing ePHI?	
	Are paper charts or portable computers/ other media containing PHI ever taken out of the office? This includes portable computers, back-up tapes, smart phones, paper charts, etc.	
	Is there a secure transport system in place? Is it consistently followed?	
	Are electronic devices encrypted? Do you periodically check electronic equipment to ensure encryption safeguards have not been disabled?	
	How does your Organization "secure" non-electronic PHI and protect oral PHI?	
Complaints and Investigations: Breach Notification		
Filing Complaints	Has your workforce been trained on the procedures for filing complaints internally and externally?	

	Is this information included in the Notice of Privacy Practices for consumers?	
Reporting Breaches/Security Incidents	Is your workforce trained to immediately report suspected security incidents/ breaches of PHI/ePHI?	
	Does your practice have a procedure in place to conduct an investigation of any suspected breaches of PHI?	
	Have you asked your Business Associates what they are doing to comply with the Breach Notification Rule?	
	Do your Business Associate Agreements to require your Business Associates to notify you promptly if they discover a breach of PHI and to provide you with all of the appropriate information regarding the breach?	
No Retaliation Policy	Has your workforce been informed that there will be no Organization retaliation for reporting a security incident/breach?	
	Does your Notice of Privacy Practices inform consumers that there will be no retaliation for reporting of complaints, security incidents or breaches to which they become aware or witness?	
Penalties	Has the Organization established sanction guidelines for workforce members that violate HIPAA policies/procedures?	
	Has the staff been trained regarding Organization sanctions and legal/federal	

	sanctions that they may incur if they violate HIPAA policies/procedures?	
	Is there consistency, aligned with policy guidelines, for the imposing of sanctions?	
Code Sets	Does your Organization follow requirements for NPI, EIN and ICD-9 CM codes?	
Notifications		
Notification to Media	Does policy establish under what circumstances media must be notified of breaches?	
	Does policy define who shall be responsible for placing media notices?	
	If media notices have been employed, did they follow regulatory requirements as set forth in policy?	
Notification of HHS	Does policy establish under what circumstances HHS must be notified of breaches?	
	Does policy define who shall be responsible for notifying HHS?	
	If HHS notice(s) have occurred, did they follow regulatory requirements as set forth in policy?	
Notification to JC	Does policy establish under what circumstances JC must be notified of breaches?	
	Does policy define who shall be responsible for notifying JC?	

	If JC notice(s) have occurred, did they follow JC standards requirements as set forth in policy?	
Notification to Business Associates	Does policy address under what circumstances and by whom Business Associates would be notified of breaches?	
	Does the Business Associate Contract direct the BA of circumstances when they must notify the Organization of breaches/security incidents?	
Notification or Delay to Law Enforcement	Does policy identify under what circumstances law enforcement will be notified and circumstances when a delay of notice is justified?	
	If such notice or delay has occurred, did it follow policy/regulations?	
Uses and Disclosures		
Permitted Use/Mandatory Disclosure	Has the workforce been trained regarding when use and disclosure may occur, under what conditions it is mandatory, and who is authorized to issue such disclosure?	
	Is a log maintained of all disclosures?	
Disclosure with and without Authorization	Has the workforce been trained regarding when disclosure requires authorization and when it does not, and who is authorized to issue such disclosure?	
	Are Release of Information Forms consistently and properly employed before the disclosure of PHI requiring authorization?	

Agreed to Restrictions	Has the workforce been trained regarding when restrictions can be placed on PHI by a consumer/guardian and who is authorized to obtain such disclosure restrictions?	
	Is there a designated mechanism for recording and notifying pertinent workforce members of any restrictions?	
Sale of PHI/ePHI; De-identified Use	Is there policy that prohibits the sale of PHI/ePHI by the Organization and its workforce?	
	Does policy stipulate the de-identification process if PHI/ePHI is used for marketing, research or related purposes?	
Notice of Privacy Practices	Is the Notice of Privacy Practices for consumers' current with regulations?	
	Is the notice being given to the consumer and discussed at intake?	

HIPAA RISK ANALYSIS REPORT

HIPAA Security requires the Agency to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic Protected Health Information ("ePHI") and to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. *This Risk Analysis is focused on doing a through and accurate assessment of all forms of PHI/ePHI used by the Agency to identify any potential risks or vulnerabilities to confidentiality, integrity, and availability of PHI/ePHI necessary to perform Agency business and document delivery of consumer care in a safe, timely, accurate and complete fashion without compromising HIPAA compliance.* ***Assessing risks is only a first step. You must use the results of your risk assessment to develop and implement appropriate mitigation activities and, as needed, revision to policies and procedures.***

Step I. Gather information on the information system (check off information reviewed):

___ Changes in media being used ___ Changes in geographical service area

___ Changes in care/service environment ___ Changes in Business Associates and Maintenance Agencies used

___ Changes in state/federal laws, regulations, or Joint Commission (JC) standards applicable to PHI/ePHI

___ Review of all reported/identified potential and/or actual vulnerabilities to confidentiality, integrity and/or availability of PHI/ePHI experienced by the Agency in the past year (review all HIPAA logs, reports, inspection results, etc.)

___ Findings from any external reviews related to HIPAA compliance

___ Other _____

Step 2. The Risk Analysis team is comprised of the Security and Privacy Officers, any Deputies, and the EMR Administrators. Others may be invited to participate fully or as needed during this analysis.

Names and Positions of Participants: _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

_____ _____ _____

Who will write up the report for submission to the Clinical Committee? _____

Date(s) Conducted: _____

Step 3. Describe/discuss the current process for each type of media that generates, stores, discloses, and/or disposes of each type of PHI/ePHI. Considering all the data you reviewed (listed earlier) and the current process, identify the level of risk for each process/sub-process to determine if changes need to be made in the process, how it is practiced, related policy, training, etc.

PROCESS/SUB PROCESSES	PROBABILITY	SEVERITY: MAGNITUDE & MITIGATION						RISK	
	Likelihood of risk	CONSUMER/STAFF CONSEQUENCE RISK	PROPERTY RISK	ORGANIZA-TION RISK	PREPARED-NESS TO INTERVENE IN NON-COMPLIANCE	INTERNAL RESPONSE	EXTERNAL RESPONSE	*Relative threat*	COMMENTS
SCORE	0 = N/A 1 = LOW 2 = MODERATE 3 = HIGH	0 = N/A 1 = LOW 2 = MODERATE 3 = HIGH	0 = N/A 1 = LOW 2 = MODERATE 3 = HIGH	0 = N/A 1 = LOW 2 = MODERATE 3 = HIGH	0 = N/A 1 = HIGH 2 = MODERATE 3 = LOW/NONE	0 = N/A 1 = HIGH 2 = MODERATE 3 = LOW/NONE	0 = N/A 1 = HIGH 2 = MODERATE 3 = LOW/NONE	0 – 100%	
Definitions of Probability: Low means we are not at risk or risk is exceedingly unlikely (ex., while a tornado could wipe out an office and its electronic equipment, we are not in a tornado zone so a tornado is unlikely); **Moderate** means that while we are not currently at risk, we could potentially become at risk if circumstances or events changed (ex., a poorly maintained inventory of electronic equipment would put us at risk of not being able to reconstruct an office for an insurance claim in the event of a disaster); **High** means we are at risk now; we believe the situation or activity could put a consumer, staff, office or the Agency at risk (ex., if a portable computer or smart phone contains scheduling or consumer information, we have a high risk of exposing consumer information if the ePHI it contains is not encrypted).									
ADMINISTRATIVE SAFEGUARDS									
Sanctions process									

Security measures enforcement									
Review of system activities regularly									
Assignment of security and privacy responsibilities									
Workforce security: supervision/access/ clearance/termination									
Information access Management: authorized access/ modification									
Security awareness and training: passwords/log-in monitoring/malware protection/reminders and training									
Security incidents/ breaches: reporting/response									
Contingency Plan: data back-up, disaster recovery/emergency mode operations/testing of each/criticality analysis									
Business Associate contracts									
Inspections/Evaluations									
PHYSICAL SAFEGUARDS									

Facility-specific security safeguards									
Maintenance records or log									
Workstation use/security									
Devise/media controls: disposal/re-use/data back-up and storage/movement log									
TECHNICAL SAFEGUARDS									
Access control: user ID/ emergency access/ automatic log-off/ encryption and decryption									
Audit controls: mechanism(s) to monitor use/activity/ authentication									
Integrity: mechanism(s) to prevent improper alterations/destructio n									
Person/Entity Authentication: knowing the right person is getting access									
Transmission security: transmitted info cannot be modified/ transmissions are									

encrypted									
COMPLAINTS AND INVESTIGATIONS									
Filing complaints: QBH, JC, HHS									
Reporting and review process									
No retaliation policy									
Penalties for violations									
Code sets: NPI/EIN/ICD-9 CM									
NOTIFICATIONS									
To media									
To HHS: <500 exposed consumers/>500 exposed consumers									
To JC									
To Business Associates									
To law enforcement/ delay of notice									
USES AND DISCLOSURES									
Permitted use									
Mandatory disclosure									
Disclosure without authorization									
Disclosure with authorization									
Minimum necessary rule									
Agreed upon restrictions									
De-identification use									
Sale of PHI/ePHI									

Notice of Privacy Practices									

RISK = PROBABILITY + RESPONSE
0.00 = 0.00 + 0.00

INSTRUCTIONS: Evaluate potential for risk and response relative to each process (some include sub-processes which you can rate individually or collectively) using the risk specific scale. Consider the data (listed earlier in this form in assigning risk/response.

Consider for ***probability***, but not limited to: 1) known risk; 2) historical risk; 3) vendor/manufacturer statistics; 4) regulatory reports/statistics
Consider for ***response***, but not limited to: 1) time to marshal an on-scene response; 2) scope of response capability; 3)historical evaluation of response success
Consider for ***consumer/staff consequence***, but not limited to: 1) volume of consumer exposure; 2) likely consequence to consumer of exposure/noncompliance if failure of the process; 3) danger of disruptions to care/service to consumer; 4) likely consequence to staff of failure in process
Consider for ***property risk***, but not limited to: 1) cost of replacement or repair if applicable to a process; 2) time to recover if process fails
Consider for ***Agency risk***, but not limited to: 1) business interruption; 2) loss of staff/consumer populations if process fails; 3) increase in external inspections with prospects of negative consequences; 5) impositions of fines, penalties, legal costs; 6) violations of contractual agreements; 7) damage to Agency reputation/ image; 8) financial burdens
Consider for ***preparedness***, but not limited to: 1) status of current policies/processes; 2) current regulatory/accreditation compliance status; 3) frequency of inspections/reviews; 4) adequacy/frequency of training to staff/deputies; 5) availability of resources needed to comply and/or respond to an issue; 6) leader support of the system/processes
Consider for ***internal response***, but not limited to: 1) internal resources' knowledge and ability; 2) EMR administrator availability; 3) clarity of roles/ responsibilities in implementation of processes and in mitigation situations; 4) timeliness of access to decision makers in mitigation situations; 5) coordination between offices and/or with home office
Consider for ***external response***, but not limited to: 1) vendor access/support/response when issues exist; 2) types of contracts/agreements for IT, maintenance and repair; 3) cooperation of vendors in sharing information/test or drill results/contingency plans; 4) coordination with other service agencies/payers/etc.

NOTE: A list of questions to help guide the review of processes is available as an addendum to this form.

Step 4. Determine processes at risk for which recommendations for action/correction are needed and determine appropriate recommendations.

List those processes that demonstrate high risk and the recommendations to be made to Clinical Committee for action/correction of risk.

HIGH RISK PROCESS	RISK SCORE	ELEMENTS AT RISK	RECOMMENDED ACTIONS

List those processes that demonstrate moderate risk and recommendations to be made to LC for decision.

MODERATE RISK PROCESS	RISK SCORE	ELEMENTS AT RISK	RECOMMENDED ACTIONS

Date submitted to LC: _____

Step 5. Summary of Clinical Committee Decisions/Actions to be taken: (Completed during Clinical Committee meeting)

AT RISK PROCESS	COMMITTEE DECISION	DATE FOR RESOLTION/RESPONSIBLE PARTY (IES)

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

PRIVACY AND SECURITY OFFICERS' EVENTS CALENDAR

AGENDA TOPIC	JAN	FEB	MAR	APRL	MAY	JUNE	JULY	AUG	SEPT	OCT	NOV	DEC
HIPAA Policies Annual Review												RV
Annual Training of Staff (may be delegated to deputy)		X										
Annual testing of Disaster Recovery Plan (Electronic Record System and Other)				X								
Annual testing of Data Back-Up Plan (Electronic Record System and Other)				X								
Annual testing of Emergency Mode Operation Plan (Electronic Record System and Other)				X								
Annual Risk Analysis	X											
Annual Applications and Data Criticality Analysis										X		
Information System Security Evaluation			X						X			
Site Inspections (can do monthly or quarterly but results reported quarterly in Security/Privacy Reports	x	x	x	x	x	x	x	x	x	x	x	x
Review of Records/Logs/Reports [Information System Activity Review]	X			X			X			X		
Review of State and Federal HIPAA Laws for changes			X						X			
Privacy Report to LC	R			R			R			R		
Security Report to LC	R			R			R			R		
Investigations of Complaints/Breaches	A/N	A/N	A/N	A/N	A/N	A/N	A/N	A/N	A/N	A/N	A/N	A/N

CODES: R= Report RV = Revisions submitted to Leadership for approval A/N = as needed X = month the activity is done; reported in next Security/Privacy Report x = option of doing activity monthly or quarterly but timely for Security/Privacy Reports

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

HIPAA SECURITY INSPECTION CHECKLIST
(Consumer is used to refer to both consumer and staff information that is considered private under state and federal privacy laws.)

LOCATION: _____ **DATE:** _____

INSPECTION ITEMS	FINDINGS/COMMENTS
VISUAL PRIVACY	
Computers have security screens and/or are kept positioned away from view of general public	
Electronic records and computer screens have a short time setting (5 min or less) to go blank or to a screensaver that will not allow re-access without a password	
All electronic sources containing ePHI, whether on site or carried by staff, have programs installed to protect from malicious software, viruses, malware	NOTE: Randomly check that the appropriate software is installed, updated and settings are proper on media. Identify program(s) in use/last update/proper settings:
SECURITY OF CONSUMER INFORMATION	
Unless encrypted/password protected, individually identifiable health information/identifiers of the individual or of relatives, employers, or household members of the consumer is not included in emails, text messages, or other unsecured sites *without decryption (i.e., removal of all possible identifiers)*	
Consumer information shared from password secured electronic sites uses only the consumer's first name if shared beyond authorized parties	
All electronic sources that contain consumer	NOTE: Randomly check electronic media for encryption during inspections.

information are encrypted: USBs, back up discs, drives, programs, networks, phones, Ipads, tablets, etc.	
No ePHI is stored on personal computers/ electronic media	
Security reminders are posted in all critical areas	
Consumer information is not distributed in any electronic format without a consumer release of information authorization, when required	
Medical Records or designee keeps a log of all releases of consumer information/ reviews of the electronic consumer record by authorized persons	
Medical Records maintains records of audit logs, access reports, security incident tracking reports and makes them available for Security Officer's review upon request	NOTE: This action may be assigned to MR staff or be retained by the Security Officer.
Procedure terminating access to ePHI is rigidly followed when employment or contract ends or other arrangements necessitating ePHI access ends	
Electronic records/profiles are not left open when the user is away from the area and/or if someone unauthorized to see the record enters the area	
Electronics that are easily removed/carried off are not left unattended and/or are locked up when not in use	

Computer workstations are not accessible to unauthorized staff, consumers or other unauthorized persons	
Passwords are assigned by CEO for each user, allowing access only to areas authorized for that user (called a profile code)	
Passwords are not shared with other staff	
Non-network Server passwords are changed with CEO initiation every 90 days	
Data back-up on encrypted disc or thumb drive occurs for all electronics with PHI or ePHI information occurs at frequency set occurs daily at end of workday	NOTE: Randomly check back-up for encryption and timely back up.
Data back-up sources are encrypted, password protected and stored securely	
Medical Records maintains an accountability record that lists movements of hardware and electronic media and change in person(s) responsible for them	NOTE: This task may be a responsibility of Dept. Directors/Supervisors/Managers for media within offices/departments.
A Security Plan is enforced to keep data, whether hard copy or electronic, secure, protected, and free from unauthorized access	
Only minimal necessary data is provided when PHI or ePHI is exchanged – applies to both data that has consumer authorization and data that does not require consumer authorization	

Disposal of electronic PHI (ePHI) and other confidential information and/or media re-use is compliant with policy	
Maintenance records are maintained of all maintenance or repair of storage areas, electronic or other equipment that contains confidential information	NOTE: This task may be a responsibility of Department Directors/Supervisors/Managers for media within offices/departments and the MR Coordinator for MR storage areas.
SECURE TRANSPORT	
ePHI is never left at an unauthorized site	
If ePHI is left at a worksite other than the agency, it is kept in a locked cabinet/drawer within a locked room whenever unattended by clinical staff	
KNOWLEDGE OF REQUIREMENTS	
Interview of staff confirms they are knowledgeable of ePHI related HIPAA and confidentiality practices of the Organization	
Staff interview reflects they are aware of the new criminal and civil penalties for failing to protect ePHI, no matter what the form in which it is maintained/ provided	
Staff interview confirms that they know who the Security Officer is and how to reach them	
Staff and manager interviews confirm that they are aware of the requirement to IMMEDIATELY report any breach of ePHI to the CEO, the Security Officer, and their supervisor	

Staff interview confirms that they know that HHS may appear at any time to conduct an audit of their PHI and ePHI HIPAA and HITECH compliance; federal law mandates such audits	
Interview of managers/ leaders reveals that they know that there must be HIPAA and HITECH specific business associate agreements with all third-party sources that have or may have access to ePHI	
Interview of staff/managers demonstrates that they know the disaster recovery plan and emergency mode operation plan for ePHI data as appropriate to their job	
EVALUATIONS	
Annual Risk Analysis of potential risks/vulnerabilities to confidentiality, integrity, and availability of ePHI	Date Done: Findings:
Annual Applications and Data Criticality Analysis to assess relative criticality of specific applications and data to support contingency plan components	Date Done: Findings:
Review of records/reports (e.g. audit logs, log in access reports, security incident tracking reports) for ePHI information system activity at least quarterly and as needed	Date Done: What Reviewed: Findings:

CONTINGENCY PLANS TESTING		
Test or oversee testing of data back-up plan at least annually at location where ePHI is used/stored (applies for All electronic documents)	Date Done: Findings:	
Test or oversee testing of the emergency mode operation plan to determine capacity to continue critical processes for ePHI while on emergency mode annually and as needed (applies for all electronic documents)	Date Done: Findings:	
Test or oversee testing of the disaster recovery plan that assesses capacity to restore any loss of data at least annually and as needed (applies for all electronic documents)	Date Done: Findings:	
TOTAL = 39	# COMPLIANT =	PERCENTAGE * =

*Divide # compliant by 39 for percentage. Provide percentage to QM Coordinator after each inspection.

- HIPAA has three components that must be addressed: privacy, security and enforcement.
- HIPAA requires safeguards of these at three levels: administrative, physical and technical.
- The new HITECH law places individuals, providers, and business associates at much greater liability with exceedingly higher penalties of both criminal and civil natures.
- The Department of Health and Human Services (HHS) has authority to do regular audits and impose civil fines, state attorneys general can file suit, and the Department of Justice can pursue criminal actions.

IF BREACH OCCURS THAT REQUIRES REPORTING TO US DEPT OF HEALTH AND HUMAN SERVICES SECRETARY, NOTIFY CEO IMMEDIATELY FOR INSTRUCTIONS.

ePHI SECURITY INSPECTION FINDINGS REPORT

==========

THIS SECTION TO BE COMPLETED BY SECURITY OFFICER

DATE OF SURVEILLANCE: _____ INSPECTOR: _____

DEPARTMENT: _____ REPORT RECIPIENT: _____

The following items related to ePHI HIPAA and Privacy/Confidentiality Practices were identified to need improvement:

1.
2.
3.
4.
5.

Were any breaches or complaints reported/identified? __Yes __No

Reported to CEO? __ Yes __ No

==========

THIS SECTION TO BE COMPLETED BY DIRECTOR/MANAGER RESPONSIBLE FOR THE AREA OF VIOLATIOINS

Please inform the Security Officer of corrective actions taken within 1 week of receiving this report. A copy of the corrective actions will be reported to the CEO by the Security Officer. Thank you for your cooperation.

	ACTION TAKEN	DATE RESOLVED
1.	_____	_____
2.	_____	_____
3.	_____	_____
4.	_____	_____
5.	_____	_____

SENT TO _____ ON: _____ BY: _____

==========

THIS SECTION TO BE COMPLETED BY SECURITY OFFICER

RECEIVED BY SECURITY OFFICER ON: _____

CORRECTIONS: ___ SATISFACTORY ___UNSATISFACTORY

ACTION TAKEN: _____

_____

SERVICE PROVIDERS LIST

Location: ______________________________ **Year:** ____________

NAME	FUNCTION A=Administrative M = Medical staff C=Clinical staff T=IT personnel M=Maintenance O=other ______	ACCESS TO: (Check all that apply)			COMMENTS (e.g. dates present; all/most work day access; 7 day/wk. access) or other pertinent info
		FACILITY	INTERNET	PHI/ePHI	

Initiated: 2/2022
Reviewed/Revised: 2/2023, 1/2024, 1/2025

Technology Use and Needs Assessment

General Needs Assessment Statement

Quality Behavioral Health, Inc., has accomplished a lot in the area of technology equipment use. QBH realizes that using technology equipment is no longer an option and we are committed to providing 21st Century tools to all staff, consumers and stakeholders. With that in mind, we have initiated the process of assessing our technology systems and equipment every three years. The focus of the assessment is to see what we are doing well and what we need to focus on for the future.

The following is the inventory of all Technology Equipment from all QBH facilities:

STERLING HEIGHTS OFFICE

Computers
1 HP Touch/Voice Smart Model No. RT3092
1 Gateway Model No. ZX4665
1 HP Model No. R15390
1 Vizio Model No. E190VA
1 Laptop HP Model No. 2B44DX
4 HP 23vx (Monitor)
1 HP 50vx (Monitor)

Printers
2 Brothers Model No. HL-2280DW
1 Brothers Model No. MFC-L2700DW
1 Xerox Model XR 10901

Tablet
1 Apple ipad Model A1416

Scanner:
1 Scan Snap Fujitsu Model No. S I500m

Phones:
8 Polycom VVX201
1 Apple 6 Cellular

TV
4 Samsung 45" Smart

Hand Held 2Way Radios
8 Midland 50 Channel Model # LXT118

Security Cameras
11

Click here to enter text.

Shredders
2 Ativa Model No. HD1600
1 Fellowex Model No. 11C4.75

DETROIT OFFICE

Scanner:
5 Scan Snap Ix500EE

Computers:
1 Acer Model No. SNID-434000
1 Acer Model No. AL-1917WL
1HP All-in-One Model No. 23-r117c
2 Gateway 42401989030 Desktop
2 Laptop HP Pavillion
1 Laptop Dell Inspiron 15
4 HP 23vx (Monitor)
1 HP 50vx (Monitor)

Tablet
1 Galaxy Model SM T350NZASXAR

Phones:
1 Polycom VVX600
10 Polycom VVX201

TV
30 SEIKI SE2HY10 TV
1 Magnavox 50" Smart

Printers:
1 Xerox Serial No. D0088
1 Xerox Serial No. D0089
2 Xerox Serial No. D0013
1 Brothers 0638 Model No. 41442 36998
1 Brothers Model No. HL-L26220D
1 Image Class Model No. MF4350 D

Hand Held 2Way Radios
10 Midland 50 Channel Model # LXT118

Security Cameras
24

Security Monitors
4 42" Split Screen

Click here to enter text.

Shredders
6 Fellowex Model No. 11C4.75

TROY OFFICE

Scanner:
3 Scan Snap I500

Computers:
7 HP Desktop Computers
3 Insignia Monitors

Tablet
1 Microsoft Surface

Phones:
8 Yealink Phones

TV
1 Samsung TV
3 Vizio TVs

Printers:
3 Kyocera Printers
5 Brother Printers
1 Dymo Lable Printer

Security Cameras

Security Monitors
4 42" Split Screen

Shredders
1 Fellowers Shredder

Other
1 Dymo Lable Printer

4 Topaz Signature Pads

1 Methadone Pump

1 Jackery Power Outdoors Generator

Click here to enter text.

Survey Findings:

All QBH Locations had adequate technology equipment to perform the best possible services for its consumers and stakeholders. Each location has adequate equipment to assure staff's work efficiency. The equipment has a variety of accessibility features to accommodate staff or consumers that might have disabilities. Some features include: talk to text, low vision monitors, phones equipped for those with hearing and visual disabilities.

The Security Team's two-way radio system functions at peck frequency, enabling the security team to communicate from both Detroit locations.

All QBH sites have adequate internet service. Each location is equipped with Wi-Fi to assure all staff, guest and consumers can use the internet as needed. The service is protected by a secured log on which is periodically updated to maintain security.

QBH has a variety of software to assure compatibility with contractors' systems and to efficiently communicate with all stakeholders.

The QBH Fire Safety System was newly updated and is directly connected to the City of Detroit Fire Department to assure fast service in the event of an emergency.

The QBH Security System consists of Security Alarms and Cameras that are monitored at 6 Security Stations. The monitoring systems are manned 24/7 to maximize the safety of our staff and consumers.

Strengths:
- E-mail system is effective.
- Systems provide accessible information through Electronic Medical Records System.
- Employees have a say in the planning and prioritizing of technology projects.
- Systems produce accurate data.
- Systems have a reliable network in place.
- Systems run on standardized desktop software.
- Departments are technology proficient.
- Voice-mail system is secure and effective.
- Individual department systems are solid and stable.

Weaknesses
- Systems are non-integrated, and data is backed up by PDF files.

Click here to enter text.

MEDICAL RECORD PEER REVIEW
MEDICAL / FORM #1
QUALITY, APPROPRIATE AND THOROUGH
LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #	
RECORDER INITIALS	

ASSESSMENT

MEDICAL HISTORY AND PHYSICAL EXAM THOROUGH

ITEM	CODE	COMMENTS
a. CHIEF COMPLAINT		
b. DETAILS OF PRESENT ILLNESS		
c. RELEVANT PAST CD TREATMENT HISTORY		
d. RELEVANT PAST MEDICAL AND INFECTIOUS DISEASE HISTORY		
e. INVENTORY OF BODY SYSTEMS		
f. REPORT OF RELEVANT PHYSICAL EXAM		
g. STATEMENT OF CONCLUSIONS OR IMPRESSIONS DRAWN FROM THE MEDICAL HISTORY AND PHYSICAL EXAM		
DIAGNOSIS OR DIAGNOSTIC IMPRESSION		
STATEMENT OF COURSE OF ACTION PLANNED FOR AND PERIODIC REVIEW		
H/P COMPLETED AND SIGNED BY LIP WITHIN 14 DAYS AFTER ADMISSION		

TREATMENT PLAN

MEDICAL RECORD PEER REVIEW
MEDICAL / FORM #1
QUALITY, APPROPRIATE AND THOROUGH
LEGEND: Y = YES N = NO NA = NOT APPLICABLE

MEDICAL RECORD #	
RECORDER INITIALS	

ITEM	**CODE**	**COMMENTS**
a. DOCTOR INVOLVED AEB SIGNATURE ON PLAN		
b. MEDICAL ORDERS REFLECTED IN PLAN		
c. PLAN ADDRESSES MEDICAL NEEDS		
d. MEDICAL TREATMENT APPROPRIATE TO LEVEL OF CARE		
e. MEDICAL TREATMENT REFLECTS CONSUMER'S NEEDS		
f. MEDICAL TREATMENT IS REVISED WHEN INDICATED		
MEDICAL PROGRESS NOTES		
ITEM	**CODE**	**COMMENTS**
a. REFLECT MEDICAL OBSERVATIONS AND RESULTS OF MEDICAL TREATMENT		
b. NOTES REFLECT MEDICAL SERVICES AS IN MEDICAL PLAN/ORDERS		
c. CONSULTATION REPORTS PRESENT IF ORDERED		
d. REPORTS OF DIAGNOSTIC AND MEDICAL PROCEDURES, LABS		
e. CONCLUSION AT TERMINATION OF SERVICES		
f. TRANSITION PLAN INCLUDES		

MEDICAL RECORD PEER REVIEW MEDICAL / FORM #1 QUALITY, APPROPRIATE AND THOROUGH *LEGEND: Y = YES N = NO NA = NOT APPLICABLE*		
MEDICAL RECORD #		
RECORDER INITIALS		
MEDICAL INSTRUCTIONS TO CONSUMER		
PSYCHIATRIC EVALUATION (AS APPLICABLE)		
HISTORY OF CURRENT PROBLEM		
MENTAL STATUS EXAM		
PAST PSYCHIATRIC HISTORY		
DIAGNOSES DETERMINED		
MEDICAL ORDERS		
ORDERS INCLUDE INDICATION/PURPOSE		
VERBAL ORDERS ARE KEPT MINIMAL		
VERBAL ORDERS ARE SIGNED WITHIN 72 HOURS		