PROCEDURES/INFORMATION SECURITY OFFICER

1) The Superintendent will designate an Information Security Officer. For the purposes of this policy, the Information Security Officer is the Information Technology Manager. The job responsibilities for this individual are detailed in this policy.
2) The Information Security Officer will be responsible for the security management process. This will include:
    A) **Information System Inventory.** The Information Security Officer or designee will maintain an inventory of the hardware, software and networking infrastructure. This will include servers, desktop computers, iPads, laptops, PDAs and any external disk drives. A copy of this inventory shall be maintained off-site to ensure availability in the event of a fire or other disaster.
    B) **Computer Security Risk Assessment**. The Risk Assessment is an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the Board. Weekly, a penetration and vulnerability test will be conducted by an outside entity to assess all Board public IP addresses. The Computer Security Risk Assessment/ vulnerability test will be managed as follows:
        a) The county board will use the risk assessment methodology detailed in NIST SP 800-30 (2001).
        b) The results of this assessment shall be documented and maintained for six (6) years.
        c) The risk assessment reports from the vendor will be reviewed as they are received. The Information Security Officer will initiate corrective action, in conjunction with other members of the management staff as necessary.
        d) The risk assessment requirements will be updated periodically.
    C) **Manage IT Infrastructure, Create and Deploy Security Policies**. On an ongoing basis, implement and maintain the IT infrastructure, draft Security Policies and write and implement procedures. More specifically, he/she will:
        a) Evaluate any regulatory requirements including HIPAA Security regulations, other applicable regulations, and industry best practices.
        b) Prepare recommendations for the Superintendent for approval by the Board including implementation of new and updated policies, acquisition of technical security measures, or physical security measures. The Board shall have final authority on risk management decisions.
        c) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with HIPAA regulations.
        d) Train Board staff regarding compliance.
        e) Monitor Board compliance with the information security policies, and take action as appropriate based on this monitoring.

1) **Data Criticality Analysis**. Data that is identified as either Critical, Important, or Non-unique, as described below, shall be backed up hourly**.** A nightly upload of critical data is performed by the Board's contracted vendor.

   A) **Critical Data:**
      a) Medicaid Billing Data
      b) Gatekeeper Information
      c) Human Resources Data
      d) Accounting Data

   B) **Important Data**
      a) E-Mail system
      b) Other Administrative Data
      c) User Directories (word processing documents, spreadsheets, other data).

   C) **Non-unique Data**
      a) Operating System, other system software, and applications software. Non-unique Data is less critical since it can be recreated by reloading from vendor supplied media, and is also backed up daily.

2) **Backup Plan.** The backup plan is a contracted service with Alphalink. Disaster recovery tests are ran quarterly to verify the offsite images. The Information Security Officer or designee is notified if there is a failure in the backup. Problems should be immediately reported to the Information Security Officer or the Superintendent if the Information Security Officer is unavailable.

3) **Data Recovery Plan.** The Information Security Officer shall maintain a written plan for restoration of data in the event of various system failures.

PROCEDURES/DISASTER, RECOVERY AND EMERGENCY OPERATIONS

1) **Scenario Identification**. Contingency planning shall begin with identification of likely failure scenarios. These scenarios include, at a minimum, failure of one or more servers, data corruption of one or more subsystems, and catastrophic loss of the entire facility due to fire or other natural disaster. These scenarios shall be included in the written recovery plan, and serve as the basis for the measures outlined below.
2) **Preventative Measures**. The Information Security Officer shall, on an ongoing basis, evaluate the activities that are critical to Board operations and implement preventative measures to reduce the likelihood of system failure.
3) **System and Data Recovery Plan**. The Information Security Officer shall maintain a written system and data recovery plan, and take reasonable steps to mitigate losses, for likely failures. The written plan shall include:

D) Computer applications shall be reviewed and assessed as to their criticality for maintaining Board operations. The results of this assessment shall be documented.
E) Development of written documentation of tasks and responsibilities for LCBDD staff with specific responsibilities in the event of likely failures.
F) System configuration documentation that facilitates replacement of vital equipment in the event of a catastrophic loss.
G) Complete and current staff information and vital records.
H) Identification of, contact information for, vendors who will be used for replacing equipment following a disaster.

4) **Reasonable steps to assure rapid recovery shall include, if appropriate:**
   A) Contracts with any necessary consultants and/or vendors to facilitate recovery, if deemed necessary and prudent by Board management.
   B) Contracts with hot and/or cold system sites if deemed necessary and prudent by Board management.
   C) Steps to manage risk, such as insurance policies, as deemed appropriate, for possible losses to mitigate the financial impact of disasters.
5) **Emergency Mode Operations Plan**. The Information Security Officer shall maintain a plan to maintain vital operations in the event of a partial or complete system failure. This should begin with an identification of likely failure scenarios as described above. Elements of this plan may include:
   A) Identification of situations which occur where immediate access to data is necessary, as in certain MUIs involving health emergencies.
   B) Maintenance of Critical Consumer Data in required case records.
   C) Notification to Service Coordinators or other individuals requiring immediate access to information in the event of an emergency for people we support (accident, medical incident, etc.).
   D) In the event of system downtime, staff will generate data on paper that will later be keyed into the system once restored.
6) **Plan Testing.** The Information Security Officer shall be responsible for plan testing. He or she shall design the approach to testing and the level of resources which are appropriate to invest in these activities based on the risk analysis.
7) **Off Site Storage of Key Documents.** A copy of the key documents described here shall be maintained off site, by the contracted computer support service in either paper or electronic form, so that they are readily and quickly assessable in the event of catastrophic loss of the facility.

PROCEDURES/FACILITY SECURITY AND ACCESS CONTROL

1) **Facility Security Planning**. The Information Security Officer shall periodically evaluate physical security vulnerabilities, identify corrective measures, and recommend to the LCBDD Safety Committee specific security measures that need to be addressed. The measures should focus especially on the security of:

A) Fire protection for server and paper PHI (protected health information), including either a fire suppression system and/or fire retardant file cabinets for paper PHI.
B) Telephone and networking equipment
C) Staff offices
D) Workstation locations
E) Case Records. Record rooms should be locked whenever possible, and cabinets that contain PHI should be locked. Attention should be given to areas with public access, whether workstations are protected from public access or viewing, the security of entrances and exits, and normal physical protections (locks on doors, windows, etc.).

2) **Staff Training.** The Component Directors, assisted by the Information Security Officer, shall be responsible for staff training on the duties and responsibilities for facility security.
3) **Maintenance of Physical Security Equipment**. Facility Maintenance personnel shall be responsible for maintaining equipment necessary to secure the facility, including locks, alarm systems, doors, security lighting, etc. Records of repairs and modifications shall be maintained.
4) **Unauthorized Individuals**. Any staff member who sees an unauthorized, unescorted person in the facility, except those in public access areas, shall politely escort the person to a common area. Any suspicious incident shall be reported to the Component Director.

PROCEDURES/ANNUAL SECURITY ASSESSMENT

1) On an annual basis the Information Security Officer will review any updates to federal HIPAA regulations, other applicable federal and/or state statues, and technological issues. The organization's Security Policy and related procedures will be updated as appropriate.
2) The Information Security Officer shall submit any recommendations in writing regarding compliance to the Superintendent.
3) These recommendations shall be retained for six (6) years.
4) A security evaluation should be conducted with the introduction of new technology, such as wireless access, etc., in response to newly recognized risks, or other events which would likely impact overall system security.
5) Weekly, a penetration and vulnerability test will be conducted by an outside entity to assess all Board public IP addresses (refer to the PROCEDURES/INFORMATION SECURITY OFFICER: Computer Security Risk Assessment section of this document).

PROCEDURES/AUDIT CONTROL AND ACTIVITY REVIEW

1) **System Activity Logs**. Activity logs shall be used at the following levels:
   A) Network Software (Windows NT): Audits will be set to log logon events, account management events, policy changes, and system events.
   B) Firewall Hardware and Software: Logs will be used to track inbound and outbound activity, including internet access by individual.

C) Application Software Logging: All software that stores data on persons served shall have audit trail capabilities. Logs will be used in application of software such as clinical record software, billing software, or client information systems.

2) **Security on Logs**. Appropriate security features and passwords will be used at all levels to permit log file access only by the Information Security Officer or designee.
3) **Audit of PHI Access**. A review of system activity will be conducted at random and will always be conducted for reasonable suspicion. The Information Security Officer shall work with the Board's contracted vendor to identify probable or anticipated violations. Suspicious and/or inappropriate activities include but are not limited to:
    a. Access by individuals at unusual hours
    b. Higher access/usage levels than normal
    c. Accesses to records of relatives of celebrities or other staff
    d. Unauthorized changes to security settings
    e. Web sites viewed by staff to verify that they are work related
    f. Outside probe attempts and/or accesses via the internet connection
    g. Other unusual patterns of activity
4) **System Activity Review.** The Information System Officer, or a designee, will monitor system activity to detect suspicious or unusual system activity.
5) **Corrective Action.** The Information Security Officer will initiate corrective action, in conjunction with other members of the management staff, in the event any inappropriate PHI access, or if suspicious or unusual system activity is detected.
6) **Purge of Log files.** System Log files which grow large may be purged under the direction of the Information Security Officer.

PROCEDURES/MALICIOUS SOFTWARE PROTECTION

1) The Information Security Officer will ensure that all computers in the facility are protected with reputable software for protection against malicious software. This software should protect against the various categories of malicious software, including viruses, Trojans, Adware, and spyware.
2) Appropriate configuration options will be established in the software to protect against malicious software contained in:
    a. Incoming e-mail and e-mail attachments
    b. Files saved to any hard disk
3) Virus protection software will be updated:
    A) Daily and
    B) At system boot
4) Periodic review of the malicious software protection will be conducted to ensure that the products, services, and configuration, and policies appropriately manage risk for any evolving threat.

PROCEDURES/SECURITY AWARENESS

1) The Information Security Officer shall develop and maintain a security-training program for new staff. This should include, at a minimum:
    A) Password practices
    B) Recognizing and avoid malicious software
    C) Understanding e-mail attachments
    D) Safe web browsing practices
    E) Dangers of downloading files from the internet
    F) Understanding of "Social Engineering" and how to recognize such ploys
    G) Knowledge of Workstation Use Practices in this policy
    H) Consequences for non-compliance
    I) Security Incident Reporting Procedures

    Other appropriate topics may be included at the discretion of the Information Security Officer. The program may be conducted one-on-one, or as a component of new staff orientation.
2) Upon initial implementation, the Security Training program will be provided to all staff. Subsequently, all new staff will receive the training.
3) Periodic security awareness training will be offered to all staff. The Information Security Officer shall develop an annual plan specifying the scope of the program; the goals; the target audiences; the learning objectives; the deployment methods; and the frequency of training. This annual plan will be a component of the Board's Annual Action Plan. Possible topics would include:
    A) Reinforcement of topics for the Security Training Program.
    B) New and "hot" information from e-mail advisories, online IT security new sites, and periodicals.

PROCEDURES/DEVICE AND MEDIA DISPOSAL AND RE-USE

1) **Media Disposal Handled by Information Security Officer**. In the event of a legitimate requirement to store data on a device such as a CD, a staff member should give it to the Administrative Assistant in his/her component who will either re-format the disk for future use or destroy it when the staff has no further need for it.
2) **Media Disposal and Re-use.**
    A) **CDs, DVDs and Tapes:** CDs, DVDs, and Tapes will be destroyed when they are no longer needed.
    B) **Hard Drives and Removable Storage Devices.** Removable Storage Devices will be reformatted prior to disposal or re-use. Hard drives will be re-formatted before assigned to a new user. Hard drives being disposed of or recycled will be made unusable.

PROCEDURES/TECHNICAL SAFEGUARDS

1) **Firewalls**. Hardware and/or software firewalls are employed to protect against network intrusions. These are configured to enforce board policy and related procedures, such as blocking of Internet e-mail sites, and other safeguards.
2) **E-mail.** Internal e-mails are transmitted over a virtual private network. Emails containing sensitive information sent to outside parties will be encrypted.
3) **Transmission Security**. Any transmission of PHI is not to be sent over an open networks. The virtual private network is to be used.
4) **Appropriate Audit Controls in Board-Used Software**. Software used by board staff will be evaluated for appropriate level of audit control, such as logging of all transactions or logging of key events such as creating, viewing, changing, or deleting PHI. In the event of deficiency of software currently in use, requests to vendors for enhancements will be made as appropriate. Appropriate audit controls will be criteria for continued use and/or procurement of any new operating or application software.
5) **Automatic Log Off**. Appropriate measures shall be taken to enable the automatic log-off provisions as determined by the risk assessment.
6) **Integrity Checks**. Automated integrity checks will be run on server data periodically and problems reported to the Information Security Officer for corrective action.

PROCEDURES/SYSTEM ACCESS AND TERMINATION

1) The Information Security Officer shall coordinate with the Component Director and Director of Human Resources to develop and maintain a list which identifies the positions and the categories of Protected Health Information to which they need access.
    A) The Information Security Officer shall utilize the security capabilities of the various network and application software systems to develop role-based "Access Profiles" for those different job descriptions. Vendors will be contacted for any enhancements necessary for appropriate implementation of these access profiles.
    B) The authority to grant access to information systems rests with the Superintendent and is delegated to the Component Directors. Implicit in a hiring decision is the provision of access to the information systems necessary for the job, as determined above based on Access Profiles for the position.
    C) In certain situations, such as when staff are assigned special projects, information access may be required beyond what the job description would dictate. In these cases, the Information Security Officer, after any necessary consultation with the Superintendent, has the authority to grant access to information systems which go beyond the standard Access Profiles described above.
    D) With the exception of the Facilities Maintenance position, all Board staff have computer access rights to PHI.

2) **System and Facility Access for New Staff**
   A) Each staff member is issued a zero client and/or iPad. If other accommodations need to be made, the request is to come from the Component Director to the IT Manager.
   B) Any computer equipment or accessories not provided by the Board are not supported.
   C) Component Directors shall direct requests for access to information systems to the Information Security Officer or his/her designee.
   D) The Information Security Officer or designee will assign new staff requiring computer access a unique network User ID and password, and/or User IDs and passwords for other application systems. Security settings appropriate for the individual will be assigned in accordance with the access profile.
   E) The Information Security Officer or designee shall communicate the User IDs and passwords in a manner that does not compromise security by revealing the passwords to another person.
   F) The Information Security Officer or designee shall configure user accounts to automatically revert the workstation to screen savers.
   G) Staff will periodically receive Security Awareness training. They will sign an acknowledgement verifying they understand the policy and procedures and will adhere to the requirements. This will be maintained in the staff member's personnel file.

3) **Password Management**
   A) The Information Security Officer or designee shall implement a mechanism to insure that all staff change their passwords at least every 90 days.

4) **Job Changes**
   A) The Director of Human Resources will notify the Information Security Officer or designee of any job changes that affect system access so that adjustments can be made.

5) **Termination of Staff**
   A) On the last day of employment, staff passwords to the network and Application Software will be changed and/or the User IDs disabled unless otherwise designated by the Component Director.
   B) For involuntary terminations, the direct supervisor is to notify the Director of Human Resources who will coordinate with the Information Security Officer so that appropriate precautions will be taken to insure the integrity and security of confidential board information. This could include such measures as:
      i. Physically escorting the individual off the premises after notifying him/her of the termination.

ii. Disabling system access as specified above on a timely basis.
iii. Requiring all staff in the individual's workgroup to change passwords.
iv. Other measures as deemed appropriate by the Information Security Officer based on the technical sophistication of the individual and perceived threat.

6) **Emergency System Access.** In the event of an emergency, such as an MUI in which immediate access to PHI is required, a staff member who does not have appropriate system permission but requires access is to obtain approval from his/her Component Director. The Component Director will contact the Information Security Officer (or designee) who will provide the necessary access on an expedited basis.

PROCEDURES/WORKSTATION/SERVER USE AND SECURITY

1) Workstation use:

A) **Job Duties.** Computer workstations including use of internal systems, e-mail, and the internet, are for use by staff to conduct their job responsibilities. These responsibilities include only matters related to the people we support: treatment, care, coordination, documentation, billing, financial accounting, internet access for matters such as access to DoDD systems, regulatory and business affairs, facilitating payment by 3rd party payers, and other matters which are specifically job related. ANY OTHER USE IS PROHIBITED.

B) **Internet Use**. Staff will limit Internet use to job responsibilities. Staff must not download, view text or images, or otherwise engage in communications that involve pornographic or racist materials; obscene material, derogatory, inflammatory or profane material; any other objectionable material. Copyrighted materials such as software or music files must not be downloaded in violation of copyright law. Staff are prohibited from both downloading and installing executable programs without the express permission of the Information Security Officer or his/her staff.

C) **E-Mail use.** Staff with Board e-mail accounts are to check e-mail daily while they are working. E-mail is to be used for Board purposes only. E-mail should be written in professional manner and should be courteous and respectful. Other requirements when using e-mail:

a. Use of e-mail internally is acceptable for transmitting PHI. Be aware that e-mail to outside parties is not secure and should be used only in limited circumstances for transmitting Protected Health Information.
b. Do not send chain letters.
c. Do not forward agency e-mail to personal e-mail accounts.
d. Limit using the "reply all" button unless you know each recipient and they have a need to know information.

e. Use only Board-supplied e-mail account. The use of internet-based personal e-mail accounts such as Yahoo, GMail, Hotmail, and MSN Mail at work is prohibited.

D) **Instant Messaging.** Instant Messaging is only appropriate for brief, internal communications. Instant messaging is not archived.

E) **BYOD (Bring Your Own Device/Personal Device Usage.)** For optimal network performance and for security reasons, staff may not connect personal devices to the Board's network without prior authorization from the IT Manager**.** In addition, staff are prohibited from using private e-mail accounts, private phone numbers or personal electronic devices to conduct Board business.

F) **Storage of PHI or Confidential Material to Removable Media Prohibited.** Staff may not copy to removable media, or transmit via e-mail or fax or other method, any board confidential information or Protected Health Information on board computer system, except when specifically authorized for Board purposes.

G) **All Usage is Logged.** THE BOARD RESERVES THE RIGHT TO MONITOR ALL USAGE OF BOARD WORKSTATIONS THROUGH THE LOGGING AND STORAGE OF ALL ACTIVITY, INCLUDING ALL E-MAIL SENT OR RECEIVED, WEB SITES BROWSED AND OTHER ACTIVITY. All logs of staff activity are property of the Board.

H) **Data Storage on Server Only.** All data must be stored on the server. Data on workstations is backed up onto the server hourly.

2. WORKSTATION SECURITY

A) Except with written approval from the Information Security Officer and Component Director, workstations must not be setup in a public access area. Staff should understand how to avoid malicious software, and must not adjust any settings on anti-virus software installed on workstations.

B) Workstation monitors that are used to access PHI are not to face in a direction that makes visual access available to unauthorized users.

C) Workstations are configured with automatic screensaver capability so that they will become inaccessible after a maximum of 20 minutes of system inactivity.

D) Employees must not install any software on their computer without authorization from the Information Security Officer.

E) All Board servers must be secured with a password and setup to automatically lock out user access after a maximum of five (5) minutes of inactivity.

F) Any network accessed by staff must be a secure network protected by a password.

3. USER IDS AND PASSWORDS

A) Staff that use workstations are assigned a unique User ID and Password. Staff will be held accountable for all system activity performed using this User ID. Inappropriate use of systems attributable to a staff member's User ID may result in disciplinary action, including termination, and in the event of violation of laws, civil and criminal prosecution. Consequently, passwords should be kept secure and confidential.

B) Passwords should be at least 6 characters long, and include at least one non-letter character. The letters should not spell a word in a dictionary or a person's name. The password should not be related to the person in anyway, as in a birth date, spouse, pet name, or anything that can be easily guessed.

C) In general, passwords should be memorized and not written, especially not in the vicinity of a workstation.

D) Users are required to change all passwords at least every 90 days.

E) Users are not permitted to allow others to access the system with their User ID and/or divulge their password.

4. EMERGENCY SYSTEM ACCESS

A) In the event of an emergency where immediate access to system information is required but not immediately possible, staff will utilize case records to access PHI. Other data will be generated in written form and later transferred to computer. Reports of Major Unusual Incidents (MUIs) will be hand written and Mid-East Ohio Regional Council (MEORC) notified by the end of the following business day.

PROCEDURES/SECURITY INCIDENT RESPONSE AND REPORTING

A) The Information Security Officer is responsible for managing security incident response and reporting. This includes mitigation strategy. The Superintendent will direct communications with law enforcement, those receiving Board services, and the media.

B) Any staff member who becomes aware of a security incident must immediately contact the Information Security Officer to report the incident.

C) The Information Security Officer and Component Director will respond to all security incidents in an expedited manner to mitigate the potential harmful effects of the security incident.

D) A written report will be completed by the Information Security Officer or Privacy Officer, within 24 hours (or as soon as possible) of becoming aware of the incident. The report should include:

1) Date and time of report
2) Date and time of incident
3) Description of circumstances and risk assessment
4) Type of Personal Health Information involved
5) Notification to the affected parties of the breach within 60 days
6) Recommended steps for the affected people
7) Corrective action taken by the Board

8) Mitigating action taken

Documentation will be kept for six (6) years.

E) The Information Security Officer and Component Director(s) will conduct a post-incident analysis to evaluate the organization's safeguards and the effectiveness of response, and recommend any changes they believe appropriate.

F) In the case of an incidental breach, no further action is required. If discovery determines there is a likelihood of harm, notifications will be made to the Superintendent, Public Information Officer, and the Licking County Prosecutor's Office immediately, but in no case later than 60 calendar days from the date of the discovery of the breach. Notification will then be made to:
   1) Affected people
   2) Providers (if applicable)
   3) Media
   4) The LCBDD website (if more than 10 people were violated)
   5) The United States Department of Health and Human Services Secretary. The notification should be made immediately if more than 500 people were violated. Notification will be made within 60 days if less than 500 people were violated. The notification to the Secretary will be via the breach report form found on the Health and Human Services web site at www.hhs.gov/ocr/privacy .

PROCEDURES/REPORTING OF VIOLATIONS

A) Any staff observing a Privacy or Security Violation is to report the violation to his/her supervisor. Failure to report a Privacy Violation is in itself a disciplinable offense.

B) The supervisor should refer the incident to the Component Director. The Component Director, with assistance from the Privacy Officer when necessary and the Information Security Officer as appropriate, will investigate the matter.

C) The Component Director and Information Security Officer, in conjunction with the staff's supervisor, will evaluate the severity of the violation, the degree of harm caused, the frequency of past violations, and the staff's overall record of performance with the board. Based on this evaluation, one or more of the following sanctions will be applied:
   1) Coaching on allowed uses and disclosures
   2) Formal warning
   3) Formal reprimand
   4) Requirement to review policies and procedures
   5) Suspension
   6) Termination

D) For grievous violations, immediate termination is generally appropriate. For other violations, because of the wide variety of types of violation possible and circumstances involved, considerable flexibility in administering sanctions is given to management.

E) The Component Director, with assistance from the Privacy Officer and others as appropriate, shall take action to mitigate the harmful effects of the Privacy Violation, if

reasonable and possible. For the purposes of this policy, "Privacy Officer" refers to the Director of Service Coordination.

F) A copy of the incident report will be provided to the Privacy Officer and filed in his/her Privacy Officer's Privacy Violations file, in the staff member's personnel file, and one will be given to the staff member.

ACTIONS TO MINIMIZE HARM

A) For 12 months following a breach, the Board will offer to pay for credit reporting for each individual whose information was jeopardized.

B) If a Business Associate made the violation, the costs associated with the breach or violation will be absorbed by the Business Associate.

ACTIONS BY THE SECURITY OFFICER TO PREVENT FUTURE OCCURANCES

A) An internal review of all applicable security policies and procedures will be conducted.

B) A full inventory of computer safeguards (hardware and software) will be completed.

C) A report to the Superintendent with recommendations and corrective actions will be completed.

PROCEDURES/SAFE GUARDING PAPER AND ORAL PHI

A) General Procedures
   1) Staff shall escort all visitors through the premises.

B) Oral Privacy
   1) Staff shall be aware of safeguarding oral communications. This includes being aware of surroundings, and using appropriate volume when speaking to prevent others from overhearing conversations.
   2) Staff should refrain from holding conversations in common areas where people supported or visitors can overhear PHI.
   3) Any staff who becomes aware of privacy issues are to inform the Component Director and the HIPAA Privacy Officer.

C) Safeguards for Written PHI
   1) Control of Individual Files
      i. Each component director in his or her respective building(s) shall be responsible for administering the records system.
      ii. Written portions of the individual's file shall be kept in a locked storage room or locked file cabinet. Only designated staff with prior approval will have access with a key and/or combination to the storage room to view records. Only these staff shall be permitted in the storage area or cabinets.
      iii. The files shall be put away promptly when not being used.
      iv. In general, files are not to be removed from premises. Exceptions to this rule will occur when files must be used off-site, such as for a school visit or for other off-site services. While away from the office, staff should use

appropriate safeguards, such as storage in a locked trunk and/or locked briefcase. Files removed from the premises should be logged on the File Removal Log. The log shall promptly be updated upon return of the file.

v. Personal appointment books or electronic calendars with names of eligible persons and their families should be safeguarded while away from the office.

2) All staff using files and other paperwork with PHI shall arrange these items so that PHI is not readily visible to others, especially in high traffic areas such as reception area.
3) Files should not be stored in areas readily visible by individuals served and/or visitors.
4) Unneeded paper documents containing PHI shall be destroyed by placing them in locked bins to be shredded.
5) When leaving for the night, all staff are to clean their desks of PHI to reduce incidental exposures to cleaning personnel and others who may use the facilities at night.
6) Staff who keep files in their offices with PHI shall store them in a locked file cabinet, or lock their office door when leaving for the day.

PROCEDURES/BUSINESS ASSOCIATE CONTRACTS

A) The LCBDD will have a written Business Associate Agreement with every Business Associate.
B) The Business Associate Agreement will provide satisfactory assurances that the Business Associate will not use or disclose the PHI of individuals served by LCBDD other than as provided in the Business Associate Agreement. The Business Associate Agreement will conform to the requirements of the current version of the Federal HIPAA regulations.
C) The Business Associate Contract may be included as an addendum or section of an existing agreement or contract.
D) In the event LCBDD learns of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate Contract, LCBDD will take steps to cure the breach or end the violation. If LCBDD is unable to cure the breach or end the violation, LCBDD will terminate the Business Associate Contract.

DEFINITIONS

Business Associate (as defined in HIPAA, 45 CFR 160.103) a person or entity who, on behalf of a Covered Entity or an Organized Health Care Arrangement, but not in the capacity of a member of the workforce, performs or assists in the performance of a function or activity involving the use or disclosure of PHI. A Business Associate includes, but is not limited to, legal actuarial, consulting, data aggregation, management, administrative, accreditation and financial services involving the disclosure of PHI.

Protected Health Information (PHI) any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR § 164.501.
Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
Privacy Violation allowed uses and disclosures of PHI are described in considerable detail in policies and procedures in this policy. For the purposes of this policy, a "privacy violation" is any use or disclosure that is not explicitly allowed in these policies.
Employee Security Procedure Violation. The failure of an employee to comply with one or more of the policies and procedures described in the HIPAA Security Policies section of the Policies and Procedures Manual.
Social Engineering – "an outside hacker's use of psychological tricks on legitimate users of a computer system in order to obtain information he needs to gain access to the system", or "getting needed information (for example, a password) from a person rather than breaking into a system." Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.
Minor Violation. A minor violation is defined as a breach of policies, due to either carelessness or ignorance, which results in minimal harm.
Intentional Violation. A breach of policies done deliberately and knowingly by an employee, but which results in no personal gain and not done for malicious intent.
Grievous Violation. A breach of policies that is done either with malicious intent or for personal gain.
Information Security Officer refers to the LCBDD Information Technology Manager.
Privacy Officer refers to the LCBDD Director of Service Coordination.