11000 SERIES SECURITY

POLICY:

Easterseals Central & Southeast Ohio, Inc. has procedures in place to ensure all employees have appropriate access to electronic protected health information (EPHI).

PROCEDURE:

1. Authorization and/or supervision

    a. This procedure is intended to cover the occasional need of workers to access EPHI. Examples would include maintenance work on computer equipment and access to offices where EPHI is maintained.
    b. The occasional access as described above must be authorized by the HIPAA Security Officer. The HIPAA Security Officer will maintain a log of all authorizations issued. The log will include names, dates, and type of access authorized.

2. Workforce Clearance Procedure

    a. As stated in the Easterseals Operations Manual, Policy #2050 Conditions of Employment, every potential employee undergoes a criminal background check, employment verification, abuser registry check, and reference checks. Employment is conditional upon the successful results of these screenings.
    b. Once hired, access to EPHI is dependent upon the position.

3. Termination Procedures

    a. E-mail for all terminated employees will be disabled upon departure from employment by the Human Resources Manager or designee. Information Technology shall be notified within one (1) business day of termination for the purpose of permanently removing employees from the e-mail system.
    b. The Human Resources Manager, or designee, will remove access to all billing and general ledger systems of any employee terminated within one (1) business day of notification.
    c. All keys, name badges, and/or credit cards issued will be collected before the end of an employee's last scheduled shift.

Originated: 3/05
Reviewed: 8/06, 8/07, 8/08, 8/09, 7/10, 8/11, 5/12, 9/15, 5/19, 6/24
Revised: 8/09, 6/24

SECURITY INCIDENT REPORTING **11100**

POLICY:

Easterseals Central & Southeast Ohio, Inc. has procedures in place to ensure security incidents are reported appropriately. The Security Officer for client-related incidents will be the Chief Operating Officer and for IT related incidents will be the Chief Finance Officer.

PROCEDURE:

1. Security incidents include all attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations of the organization's information systems.

2. If an employee becomes aware of a security incident, the Security Officer should be notified immediately.

3. The Security Officer will convene and inform the appropriate Recovery Team members of the incident.

4. The Team will determine what impact the incident has had on systems and will use the Disaster Recovery Manual as a guide to proceed through appropriate recovery plans.

5. The Incident will be recorded on a Security Incident Reporting form.

Originated: 4/05
Reviewed: 8/06, 8/07, 8/08, 8/09, 7/10, 8/11, 5/12, 5/19, 6/24
Revised: 9/11, 9/15

POLICY:

Easterseals Central & Southeast Ohio, Inc. has procedures in place to ensure proper control over access to all physical facilities.

PROCEDURE:

1. Contingency Operations

   Highlighted in the Information Technology Systems Recovery/Emergency Mode Operation Manual and in the Business Continuity Manual are actions to be taken to ensure operations can continue in the event of a disaster. Actions are dependent upon the type and scope of disaster, however, if necessary; IT Consulting Firm data center will be used as an offsite location to ensure continuing operations.

2. Access Control and Validation Procedure

   It is the responsibility of the Program Manager at each office to work in conjunction with Human Resources to assure that staff-issued keys and or name badges are relinquished in a timely manner upon termination of employment of any staff person, and that security codes and passwords are revised periodically.

3. Facility Security Plan

   A record, along with company property agreements, will be maintained by Human Resources to track the allocation of keys and security passwords for each facility. This record will list the name of each staff person who receives a building entry code or password, or any type of key. The tracking system will include the date the key or code was given, the usage of the key (e.g. master key, office key, medical records, and server room) and the dates that any codes or keys are relinquished. This list is maintained and monitored by the following staff at each facility:

   Central Ohio Office: Human Resource Manager
   Shawnee Regional Office: Community Service Manager South
   Lawrence County Office: Community Service Manager Southeast
   Northern Office: Community Service Manager

4. Maintenance Records

A staff person at each facility is designated to maintain an on-going record of any repairs and modifications made to any doors, locks, security systems, etc. This record will include the name of the item repaired or modified, a brief description of the repair or modification, and the date it occurred. The following staff at each facility is responsible for this monitoring:

Central Ohio Office: Human Resources Manager
Shawnee Regional Office: Adult Inclusion Coordinator
Lawrence County Office: Adult Inclusion Coordinator
Northern Office: Adult Inclusion Coordinator

Originated: 4/05
Reviewed: 8/06, 8/07, 8/08, 8/09, 7/10, 8/11, 5/12, 5/19, 6/24
Revised: 8/08, 8/09, 9/15, 5/19, 6/24

WORKSTATION USE AND SECURITY **11200**

POLICY:

Easterseals Central & Southeast Ohio, Inc. has procedures to ensure workstations are appropriately used and secured.

PROCEDURE:

1. Workstations will be configured based on the needs of the position using them (Appendix C).

2. Workstations will be placed in rooms so that either the monitors are not easily seen or the monitor will be equipped with a privacy screen.

3. All access to the Easterseals server will be password protected.

4. All employees must log off their computers at the end of the day and anytime they will be away from their workstations for longer than 15 minutes.

Originated: 4/05
Reviewed: 8/06, 8/07, 8/08, 8/09, 7/10, 8/11, 5/12, 9/15, 5/19, 6/24
Revised: 8/08

DEVICE AND MEDIA CONTROLS 11250

POLICY:

Easterseals Central & Southeast Ohio, Inc. has procedures in place that govern how hardware and electronic media that contain electronic protected health information (PHI) are brought into or removed from the facility and how those same things are moved within the facility.

PROCEDURE:

1. Disposal

    a. PHI on electronic media will be wiped clean before disposal. This action will be the responsibility of the Security Officer (Security Officers assignments are outlined in section 11100).
    b. Disposal of computer equipment will be the responsibility of the Security Officer. The Chief Finance Officer, or designee, will assure that all EPHI is wiped from the equipment and that disposal is accomplished in a safe and legal manner. Assistance from the organization's computer consultants will be considered in such disposals.
    c. EPHI on paper will be shredded before disposal.

2. Media Re-use

    a. All media will be wiped clean before being re-used.

3. Accountability

    a. Annual inventories of computer hardware will be prepared. These inventories will be the responsibility of the Security Officer/CFO.

4. Data Backup and Storage

    At the time of moving electronic hardware on which is resident EPHI, special consideration will be made for backing up the EPHI before the move is made. This will be considered on a case-by-case basis after evaluating the probability of loss or corruption of the information.

    Originated: 4/05
    Reviewed: 8/06, 8/07, 8/08, 8/09, 7/10, 8/11, 5/12, 6/17, 5/19, 6/24
    Revised: 9/15, 6/17

MECHANISM TO AUTHENTICATE ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI) **11300**

POLICY:

Easterseals Central & Southeast Ohio, Inc. has procedures in place to ensure protection from improper alteration or destruction of EPHI.

PROCEDURE:

1. Easterseals Waiver billing:

    a. Billing is entered into software that is then transmitted through the internet to the appropriate agencies, such as, Ohio Department of Developmental Disabilities (OD/DD) or the appropriate Area Agency on Aging (AAA).

    b. Billing entered is balanced against paper time sheets and a computer billing report is generated when billing is completed.

    c. A receipt is received confirming amount of deposit to Easterseals account.

Originated: 4/05
Reviewed: 8/06, 8/07, 8/08, 8/09, 7/10, 8/11, 5/12, 9/15, 5/19, 6/24
Revised: 8/07, 8/08, 7/10

RECORDING DEVICES **11400**

POLICY:

No recording devices are to be used in a meeting of Easterseals employees without the knowledge and consent of all parties involved in the meeting.

PROCEDURE:

Information shared in meetings is often of a confidential nature. This includes information about Easterseals Central & Southeast Ohio, Inc. business practices, and patient/client information protected by our Privacy Policy and by HIPAA. Without the knowledge and consent of all parties involved for recording to take place, the risk of a breach of confidentiality is too great.

If a party involved in a meeting wishes to record that meeting either by audio or video, every party involved in the meeting must give verbal consent to the recording.

For meetings that involve highly confidential or private information, consent for recording must be obtained in writing from each party taking part in the meeting.

The following meetings may be recorded, and attendees give their consent to be recorded by attending:

1. Board Meetings
2. Policy Committee Meetings
3. Senior Leadership Meetings
4. Program Committee Meetings
5. Health and Safety Committee Meetings

Originated: 11/13
Reviewed: 11/13, 9/15, 5/19, 6/24