Elizabeth Richardson Center
HIPAA: Policies & Procedures

HIPAA Policies & Procedures

I. Scope

- Since ERC is considered a health-care facility, all employees must abide by the Federal Law known as HIPAA (Health Insurance Portability and Accessibility Act).

II. Table of Contents for these policies & procedures

III. Release of Confidential Information Policy & Procedures

A. **Policy**

1. It is the policy of ERC that no employee will disclose any personal, medical or financial information about any individual served unless express written permission has been granted by ERC senior management.
2. It is the policy of ERC that no confidential information shall be released unless express written permission has been granted ERC senior management.

B. **Procedures**

1. All persons authorized to release medical records and information must read, understand, and comply with this policy.
2. All release of information requests must be completely filled out that also includes specific information to be released and to whom it will be released and the date(s) that cover when this information may be released ERC shall follow all state and federal laws regarding release of confidential information.

IV. POLICY - Security and Acceptable Use of Technology

A. Policy

1. All employees, contractors and volunteers (hereafter referred to as "personnel") must preserve the security, integrity and the confidentiality of all confidential and other sensitive business information pertaining to ERC's clients and business.
2. Personnel shall collect information only for the purposes of providing services and for supporting the delivery, payment, integrity, and quality of those services offered by ERC in compliance with all state and federal laws.
3. All technology equipment owned, leased and operated by ERC shall only be used for acceptable business duties by employees, contractors and volunteers of ERC. Definitions of what is acceptable and unacceptable are found later in this document.
4. All breaches of security shall immediately be reported to his or her superior, Program Director, Corporate Compliance Officer (Cathy Obana), or the Director of Human Resources. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

B. Unacceptable Use of Technology

1. The following activities are considered unacceptable uses of technology.
2. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a computer if that computer/user is disrupting network/internet services).
    a. No ERC employee should ever engage in any activity that is illegal under local, state, federal or international law while utilizing ERC-owned resources.
    b. Violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by ERC.
    c. Make an unauthorized copy of copyrighted material including, but not limited to, digitization/distribution of photographs from magazines, books or other copyrighted sources, copyrighted music.
    d. The installation of any copyrighted software for which ERC or the end user does not have an active license is strictly prohibited.
    e. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question. That includes uploading malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
    f. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
    g. Using an ERC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
    h. Making fraudulent offers of products, items, or services originating from any ERC account.
    i. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

j. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties, For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
k. Port scanning or security scanning is expressly prohibited unless prior notification is made.
l. Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.
m. Circumventing user authentication or security of any host, network or account. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack). Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
n. Providing information about or lists of ERC consumers, families, donors, mailing lists or employees to parties outside ERC.
o. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
p. Unauthorized use, or forging, of email header information or the solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies or creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
q. Use of unsolicited email originating from within ERC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by ERC or connected via ERC's network.
r. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3. For security and network maintenance purposes, authorized individuals within ERC may monitor equipment, systems and network traffic at any time, per ERC's Audit Policy. ERC reserves the right to audit networks and technology systems on a periodic basis to ensure compliance with this policy.
4. From time-to-time, technology equipment and systems may be moved, added purchased, changed or altered to meet the needs of ERC staff and consumers ONLY after getting pre-approval from ERC's Systems Administrator or designee. All additions, moves, changes or alternations must be evaluated by the Systems Administrator to ensure proper access to ERC technology equipment while maintaining the security of the ERC technology systems.
5. Acceptable Security and Proprietary Information Security

a. The information contained on Internet/Network-related systems should be classified as either confidential or not confidential, as defined by ERC confidentiality guidelines, details of which can be found in Human Resources policies.
    i. Examples of confidential information include but are not limited to: consumer and staff health related information covered by HIPAA, company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and donor lists.
    ii. Employees should take all necessary steps to prevent unauthorized access to this information.
b. Personnel shall keep passwords secure and shall not share with unauthorized users. Authorized users are responsible for the security of their passwords and accounts.
    i. System level passwords should be changed on a regular basis.
    ii. User level passwords should be changed every six (6) months.
c. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the computer will be unattended.
d. Information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
e. Virus Software
    i. All computers used by the employee that are connected to the ERC Internet/Intranet/Network, whether owned by the employee or ERC, shall be continually executing approved virus-scanning software.
    ii. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

V. Access to ERC Technology Systems Policy and Procedures

A. Policy
    1. It is the policy of ERC to have a secure technology system and to only allow access to personnel on a "need to know" basis. Data users must comply with the following requirements:
        a. Use the data only for purposes authorized by ERC.
        b. Comply with all policies and procedures governing information promulgated by ERC.
        c. Not disclose data unless authorized to do so.

B. Procedures for Approving Access to Technology Systems
    1. Program Directors or COO will submit names of personnel needing access, or modifying existing user's access to the compliance officer.
    2. Program Directors or COO will recommend levels of access needed and will ensure that all prospective data users receive required training and supervision.
    3. The Compliance Officer will grant requests in accordance and forward the request to the systems administrator to establish and assign access.

4. The compliance officer and/or the systems administrator will take the following steps:
    a. Assign the user unique user identification.
    b. Assign the user an initial password. The user will be prompted to change password during initial log in.
    c. Provide security training to all new employees that include giving new employees a copy of the policies.
        i. New employees shall sign the ERC Security Compliance Sign-off Form during New Employee Orientation and annually thereafter.
        ii. A copy of the form shall be retained in the employee's training file for six (6) years.
    d. Users will be prompted to change passwords every 6 months.
    e. Provide emergency override access for necessary personnel as determined by department heads.
    f. Suspend access when appropriate to respond to a breach of confidentiality/security in coordination with ERC's policies and procedures.
    g. Modify access when notified to do so by compliance officer or program director or HR if the staff member changes positions.
5. The Director of Human Resources is responsible for notifying the Systems Administrator and Corporate Compliance Officer of employees and others, such as independent contractors, who will be leaving ERC's employ or otherwise (through reassignment, extended absence, and so forth) and will no longer need access to technology systems/information.
    a. The Systems Administrator shall terminate access when notified to do so by the compliance officer, program director or human resources.
    b. Upon termination of an employee or other person with access, the Systems Administrator will immediately take the following actions:
        i. Revoke access privileges, such as user-IDs and passwords, to system and data resources and secure areas.
        ii. Retrieve all hardware, software, data, and documentation issued to or otherwise in the possession of the data user.
        iii. Keep records of the termination procedure for each such person, including the retrieval of security-related items, such as passwords, and information system assets, for not less than six (6) years from the termination date.
6. When necessary, the Executive Director or designee will arrange for security escort of terminated personnel from the facility and for an immediate audit of their accounts to detect any security or confidentiality threats or breaches.

C. Procedures for Approving Outside Entity Access to Therap.
    1. Program Directors and C.O.O. will determine which personnel and outside entities get access to information and systems in accordance with this Policy.
    2. In making such determinations, Program Directors will follow these guidelines:
        a. Prospective data users will not get access unless they have a need for access.
        b. Prospective data users will get only the minimum access necessary to perform duties requiring such access.

c. Health Care providers, contractors and volunteers shall have access only to data of clients for whom they have client responsibility, with an emergency override to access other clients' data to respond to emergencies.
d. Access should be limited to necessary tasks, such as read-only, read and copy, read and edit.

VI. Employee Access to PHI Policy & Procedures

A. Policy
1. It is the policy of ERC that personnel shall have access to confidential information on a "need to know" basis. ERC's employees shall be granted access to Protected Health Information (PHI), whether written, electronic or verbal in nature, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and other state and federal laws.
2. Such access shall be limited to the minimum necessary amount of PHI to accomplish the purpose of any requested use or disclosure of PHI, e.g. to the amount of PHI the employee needs to know in order to accomplish their job or task.
3. In addition, communication between employees which involves PHI shall also be considered confidential and should not take place in public areas. If it is absolutely necessary to conduct such conversations in public areas, reasonable steps shall be taken to assure the confidentiality of PHI.
4. Client PHI should never be removed from ERC's facility without specific authorization from ERC's Privacy Officer or designee. ERC shall establish a procedure for how employees or contract workers are to physically access PHI in medical records (Le, how to sign records in and out and under what conditions, etc.).
5. If PHI in any form is lost or stolen, ERC's Compliance Officer or designee shall be notified as soon as practical, but no later than 24 hours after the loss is discovered, in order for the Compliance Officer or designee to initiate remedial action.

B. Procedures
1. Facility Access
   a. Access to ERC facilities by employees and contract workers is allowed on normal workdays that may include holidays and weekends based on the program, facility and type of service provided. Access to ERC facilities beyond normal hours would require senior management approval.
   b. Only authorized employees who have been assigned an ERC name tag or visitor's badge are allowed access to ERC secure areas.
   c. ERC provides designated employees and other authorized individuals with keys and combinations necessary to access appropriate ERC facilities. Individuals who have **not** been provided with these access tools and information are to be allowed access to ERC facilities only with the advance approval of the Program Director over that facility.
2. PHI Access
   a. ERC has job descriptions that describe the duties and requirements that include access to protected client information.
3. Training

   a. ERC's employees shall be informed of their obligations with respect to PHI by mandatory participation in ERC Security Training as required by the Health Insurance Portability and Accountability Act (HIPAA).

4. Required Security Policy Compliance Agreement
   a. ERC's employees that receive or maintain PHI shall be required to agree to the protection of such PHI.
   b. All ERC employees shall sign the ERC Security Policy Compliance Form. A copy of the signed Security Policy Compliance Form shall be maintained in their training file.
5. Visitors
   a. All visitors to ERC's facilities are required to sign in on the "ERC Visitors Sign in Register" form located at the main entrance of each facility. The visitor's sheet shall have the following statement on each visitor sign in register "The Elizabeth Richardson Center (ERC) is required by the Federal Law known as HIPAA to safeguard the privacy of the individuals that we serve. As a visitor to any ERC facility, we trust that you will honor the confidentiality of the clients who live, work and go to school at our ERC facilities."
   b. All visitors shall wear a visitor's badge that they receive when they enter the facility. In the case where a badge is not available and cannot be obtained, an employee must accompany visitors while in the secured area of the facility.
6. Volunteer/Observer
   a. All volunteers (including members of the ERC Board of Directors) and/or observers at ERC shall agree to follow the policies that govern ERC.
   b. All volunteers/observers are required to sign the "Volunteer/Observer Statement of Agreement."
   c. All volunteers/observers are required to sign in and out on the Volunteer /Observer Sign-In sheet every time they enter/leave an ERC facility.
7. Suspicious Individual in a Secure Area
   a. Any employee who observes an unknown individual in a secure area who is not wearing an ERC name tag or ERC visitor's badge shall:
      i. Politely request the person's name and their affiliation with ERC;
      ii. If the person is not an employee, volunteer, intern or have a valid reason for being in that area, ask the name of the person with whom are they visiting/working;
      iii. If possible, verify with that employee that this person is an invited guest and escort them to the employee's office or work area; or
      iv. Escort the person out of the secured area and notify supervisor.
8. Lost External Access Key Procedure
   a. An employee who loses an external access key or other tool that grants access to a secure area shall:
      i. Report the key or external access tool loss to the Maintenance Coordinator as soon as possible.
      ii. Report the loss to their supervisor or program manager.
      iii. Obtain a replacement access key or other tool from Maintenance Coordinator.

iv. To the extent possible, determine the cause of the key or access tool and provide suggestions to prevent a reoccurrence.

VII. Email Policy & Procedures

A. Policy

1. It is the policy of ERC that all email sent through ERC technology systems will comply with ERC's Acceptable Use of Technology Policy.
2. ERC encourages the use of the ERC internet/network or computer-generated communication to increase productivity hereafter called "email."
3. All messages generated by or handled by the internet/network, including back-up copies, are part of the business equipment of ERC, are owned by ERC, and not the property of the users of the system.
4. Because Outlook is not a secure form of communication, no emails should be sent that contain any PHI regarding any individual receiving services at ERC. This includes texts or any other form of electronic communication except on Therap.
5. ERC employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. ERC may monitor messages without prior notice.

B. Email Procedures

1. To ensure compliance with this policy, email shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
2. Employees who receive any emails with this content from any ERC employee should report the matter to their supervisor immediately. (See definitions of email.)
3. All personnel shall exercise utmost caution when sending any email from inside ERC to an outside network or computer and within the Therap system.
    i. Unless approved by a Program Director, ERC email or S-comm's may not be automatically forwarded.
    ii. Unauthorized disclosures or sensitive information will not be forwarded via any means unless that email is critical to business and or services being offered by ERC and the individuals receiving the email have right-to-know privileges.
    iii. Using a reasonable amount of ERC resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.
4. All email other than Therap shall include the following confidential statement at the bottom of the email signature.
    i. "Confidential Statement. This e-mail transmission, and all documents, files, or previous e-mail messages attached to it may contain information that is confidential or legally privileged. This transmission is intended solely for the exclusive use of the named recipient ("intended recipient"). If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that you must not read this transmission and that any

disclosure, copying, printing, distribution, or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED. If you have received this transmission in error, please immediately notify the sender by telephone or return e-mail and delete the original transmission and its attachments without reading or saving in any manner. Thank you."

6. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

C. Securing E-PHI when using Email
   1. Currently, ERC does not have a way for employees to encrypt email that contains e-PHI going outside of the organization.
   2. Procedures to follow to limit the risk of a breach:
      a. Don't email e-PHI if you don't have too.
      b. Send only the minimum necessary.
      c. Include ERC's confidentiality statement in the signature of your email. Contact the Corporate Communication Director if you need a copy.
      d. If this is someone that you regularly correspond with by email or you are responding to an email request – bring up a previous email and respond to it. This will ensure that the email address for that person is correct.
      e. If this is a new contact and you do not have any emails from them, send a test email and ask them to respond to ensure that you have the correct email address.

VIII. Faxing Policy & Procedures

A. Policy
   1. It is the policy of ERC that all faxes sent and received shall be handled safely and securely.
   2. Confidential information may be transmitted by facsimile only when urgently needed for client care or required by a third-party payer and other more secure systems are not available.
   3. Information transmitted must be limited to that necessary to meet the requester's needs.

B. Procedures
   1. The cover page accompanying the facsimile transmission must include the confidentiality notice is part of the cover page and includes the following statement;
      a. "**IMPORTANT:** This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If you are not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that nay disclosure, copying or distribution of this information is **Strictly Prohibited**. If you have received this message by error, please notify the sender immediately to arrange for return or destruction of these documents."
   2. Reasonable efforts must be made to assure the facsimile transmission is sent to the correct destination.

3. For a new recipient, the sender should attempt to verify the fax number before sending the facsimile and verify the recipient's authority to receive confidential information.
4. Fax machines must be located in secure areas, and the program director is responsible for limiting access on a need-to-use basis.
5. Each program location is responsible for ensuring that incoming faxes are properly handled.
6. When possible, it is preferable for faxes to come in to ERC facilities electronically and be forwarded electronically so that hard copies are never printed out until they reach the intended recipient. Incoming faxes are sent directly to a folder on the network and the designated staff person moves document from folder to appropriate network folder or emails the electronic fax to the ERC staff who is the recipient of the fax.
7. Any misdirected faxes must be reported to the privacy officer immediately.
8. The program director or designee will periodically ensure that all speed-dial numbers are current, valid, accurate, and authorized to receive confidential information.
9. Users must immediately report violations of this policy to their program director or compliance officer.

IX. Audit Policy & Procedures

A. Policy
   1. It is the policy of ERC that all ERC technology systems shall have a regular technology audit using qualified internal and/or external personnel. This access may include:
      a. User level and/or system level access
      b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on ERC equipment or premises
      c. Access to work areas
      d. Access to interactively monitor and log traffic on ERC networks.

B. This policy covers all computer and communication devices owned or operated by ERC.

C. This policy also covers any computer and communications device that are present on ERC premises but which may not be owned or operated by ERC.

X. Data Back-up Policy & Procedures

A. Policy
   1. It is the policy of ERC to do a complete daily back-up of all information stored on ERC's server. This policy supplements the facility's overall security policy, which is intended to protect confidentiality, data integrity, and availability. The systems administrator or designee is responsible for implementing the Data Backup Plan.

B. Procedures
   1. ERC shall contract with a data back-up provider to complete a daily backup of all ERC shared and network drives during the overnight hours and send a report to the systems administrator.

1. The Systems administrator shall validate the backup with a network log in the system administrator's office. The system administrator will maintain such reports for a minimum of three (3) years.
2. Any errors will be reports to COO and acted upon immediately. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
3. Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
4. All personnel who detect or suspect a data backup problem should immediately report the same to the privacy officer or systems administrator. Such personnel should follow up immediate notification by noting the situation on a form provided by the privacy officer.

XI. Emergency Access Policy & Procedures

A. Policy
   1. It is the policy of ERC to allow emergency personnel access to ERC technology systems or information when an emergency arises and requires extraordinary measures to correct emergency situation.
   2. The Executive Director or designee may invoke these Emergency Access Procedures when an incident occurs that has disabled or will disable, partially or completely, the central computing facilities of ERC, the health information system, and/or the communications network for a period of four (4) hours or longer or when an incident has substantially impaired the use of computers and networks.

B. Emergency Access Procedure
   1. When such incidents occur, with the approval of the Executive Director or designee shall allow ERC personnel or other personnel, such as vendor maintenance technicians, to have access to the technology systems or its data that has not previously been granted under ERC's Access Policy to address/correct the emergency.

XII. Destruction Policy & Procedures

A. Policy
   1. It is the policy of ERG that designated personnel shall destroy data that is no longer necessary to retain.
   2. ERC Personnel shall not destroy data that is involved in audit, investigation, or litigation.

B. Procedures
   1. Executive Director or designee shall designate personnel responsible for destroying data. All personnel of ERC's must destroy data as follows:
   2. Paper records must be shredded.

3. Computers, hard drives and/or magnetic media must be degaussed upon disposal or otherwise disposed of in a manner approved by the compliance officer.

XIII. Investigation of Technology Violations Policy & Procedures

A. Policy
   1. It is the policy of ERC to investigate violations of ERC Security and Acceptable Use of Technology Policy and Access to Technology Policy.

B. Procedure
   1. Individuals detecting or suspecting a violation ERC Security and Acceptable Use of Technology Policy and Access to Technology Policy must report the breach or suspected breach to the Program Director, Compliance Officer or Human Resources as soon as possible.
   2. Depending on the violation, the Compliance Officer or Human Resources will investigate.
      a. The Compliance Officer will investigate all technology and client confidential information breaches.
      b. The compliance Officer may assist Human Resources when technology equipment or systems are used to violate staff confidential information.
      c. Human Resources will investigate all breaches of confidential information breaches by ERC staff.
   3. Upon receiving the report, the primary investigator shall will take the following steps:
      a. Take any necessary immediate corrective action to protect the integrity of the equipment, system or information.
      b. Gather information and interview appropriate personnel.
      c. All ERC personnel shall cooperate with all investigations. Failure to cooperate or furnish required information, or making false information may result in employee discipline up to and including termination.
      d. Summarize the finding of investigation
         i. Seriousness of the violation/breach
         ii. Results of the violation/breach
         iii. Corrective action taken
         iv. Corrective action needed to prevent future violations
         v. Recommendations for personnel action
      e. The Executive Director may consult legal counsel to review the report and its recommendations for legal sufficiency.
      f. The compliance officer will keep all such reports for not less than six (6) years from the date of the report.
      g. No such report will be made a part of a client's medical record. The report is a risk management tool, not a client care document.

XIV. Social Media/Networking Policies & Procedures

A. Policy
   1. Whether using ERC's property and systems or personal computer systems, personnel are also subject to the terms and restrictions set forth in this Policy.
   2. Limited and occasional use of ERC's systems to engage in social media /networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate ERC's policy, is not detrimental to ERC's best interests, and does not interfere with an employee's regular work duties.

B. Procedures
   1. Social media/networking done on ERC's technology systems is subject to monitoring.
   2. Personnel are prohibited from revealing any ERC confidential or proprietary information, trade secrets or any other material covered by ERC's Confidential Information policy when engaged in blogging.
   3. Personnel shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of ERC and/or any of its employees.
   4. Personnel are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by ERC's Non-Discrimination and Anti-Harassment policy.
   5. Employees may also not attribute personal statements, opinions or beliefs to ERC when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of ERC. Employees assume any and all risk associated with blogging.
   6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, ERC's trademarks, logos and any other ERC intellectual property may also not be used in connection with any social media/networking activity.

XV. Search Warrant Policies & Procedures

A. Policy
   1. It is the policy of ERC to release records when so required by law and will cooperate with lawful searches but will protect confidential information, such as client information and legally privileged information, to the extent authorized by law.
   2. ERC and its personnel will not attempt to obstruct an investigation or destroy, alter, or conceal documents or other evidence sought in an investigation.

B. Procedures
   1. Upon receipt of any request or subpoena for records from any governmental agency, all employees must immediately call the executive director or designee.
   2. The Executive Director may consult with ERC legal counsel, as needed. Standard requests from the Social Security Administration for information used for SSI and SSDI determination may be processed using the "Release of Information Policy and Procedures".
   3. All supervisors are responsible for enforcing this policy.

4. Employees who violate this policy are subject to discipline up to and including termination. In addition, improper interference with a search may constitute the crime of obstruction of justice, a charge that could lead to arrest and prosecution.

I. Review/Revision/Approval Information

- List previous Board approval dates and all review/revision dates made by P&P Review Committee: 4/2014, 6/2015. Procedures only changed 4/2016.
- Program managers have reviewed and approved on 4/14/2016
- Approved by Board of Directors Committee: Most current date N/A
- The Director of Administration has reviewed and approved these policies & procedures:

Lynne Keller, Director of Administration — Date 4/14/2016

- ERC Board of Directors has approved these policies on: N/A

NOTE: These policies/procedures are in the process of being extensively revised. 6/2017

☐ CARF standard(s) (Commission for the Accreditation of Rehabilitation Facilities)_____

☒ DDS regulation(s) (Dept. of Disability Services – State) 401.F, 802.1.D

☒ OLTC regulation(s) (Office of Long Term care – State) 308.1

☐ Medicaid regulations (Federal/state) _____

☒ HIPAA Regulations (Federal) Multiple

Printing this document may make it obsolete. For the latest version of this policy, always check the ERC website at www.ercinc.org/AboutUs/Policies .