Elizabeth Richardson Center
ERC Enhancing lives
Removing barriers
Creating opportunities

IF YOU ARE PRINTING THIS FROM OUR WEBSITE – this is for all staff! Please print the entire document and read it. Then sign the last page and forward just the signature page to Lynne Keller. The rest of these policies and procedures are for you to keep for your reference.

ERC HIPAA and Security Policies

Release of Confidential Information Policy

It is the policy of ERC that no employee will disclose any personal, medical or financial information about any client served unless express written permission has been granted by the client, the client's representative and ERC senior management.

It is the policy of ERC that no confidential information shall be released unless express written permission has been granted ERC senior management.

- All persons authorized to release medical records and information must read, understand, and comply with this policy.
- 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.

Security and Acceptable Use of Technology Policy

It is the policy of ERC that all employees, contractors and volunteers hereafter known as "personnel", must preserve the security, integrity and the confidentiality of all confidential and other sensitive business information pertaining to our clients and business.

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.

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.

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.

Unacceptable Uses of Technology

The following activities are, in general, prohibited. 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).

1. Under no circumstances is an employee of ERC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing ERC-owned resources.
2. Violations of 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.

3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ERC or the end user does not have an active license is strictly prohibited.
4. 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.).
5. 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.
6. 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.
7. Making fraudulent offers of products, items, or services originating from any ERC account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification is made.
11. 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.
12. 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.
13. Providing information about or lists of ERC consumers, families, donors, mailing lists or employees to parties outside ERC.
14. 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.
15. 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.

16. 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.
17. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Access to ERC Technology Systems Policy

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:

- Use the data only for purposes authorized by ERC.
- Comply with all policies and procedures governing information promulgated by ERC.
- Not disclose data unless authorized to do so.

Workforce Access to PHI Policy

It is the policy of ERC that personnel shall have access to confidential information on a "need to know" basis. ERC's workforce members 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.

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 or workforce member needs to know in order to accomplish their job or task. In addition, communication between workforce members 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 the PHI.

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 workforce members are to physically access PHI in medical records (Le, how to sign records in and out and under what conditions, etc.).

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.

Email Policy

It is the policy of ERC that all email sent through ERC technology systems will comply with ERC's Acceptable Use of Technology Policy.

- ERC encourages the use of the ERC internet/network or computer-generated communication to increase productivity hereafter called "email."
- 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 are not the property of the users of the system.
- 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

Faxing Policy

It is the policy of ERC that all faxes sent and received shall be handled safely and securely.

- 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 ore not available. Information transmitted must be limited to that necessary to meet the requester's needs.

Audit Policy

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:

- User level and/or system level access
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on ERC equipment or premises
- Access to work areas
- Access to interactively monitor and log traffic on ERC networks.

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

Data Backup Policy

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.

Emergency Access Policy

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.

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.

Destruction Policy

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

Investigation Technology Violations Policy

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

Blogging

Blogging by employees, whether using ERC's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of ERC's systems to engage in blogging 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.

Employees 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. Employees 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.

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.

Security Definitions

Affdavit: In this context an affidavit is a sworn statement detailing the probable cause for a search warrant. Probable cause consists of facts and circumstances making it more likely than not that evidence, contraband, or fruits of a crime are in the particular place to be searched.

Blogging (Writing a blog): A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Client (or Consumer): Any individual who has received or is receiving services from ERC.

Corporate Compliance Officer: The person officially designated to oversee all ongoing activities related to the development, compliance, implementation, maintenance of, and adherence to the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state laws that may apply.

Email: The electronic transmission of information through a mail protocol such as Microsoft Outlook, Therap, SEAS, any web-based email program, instant messaging systems or cell phone texting.

> **Chain email** or letter email sent to successive people: Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
>
> **Forwarded email:** Email resent from an internal network to an outside point.
>
> **Spam**: Unauthorized and/or unsolicited electronic mass mailings.

E-PHI (Electronic Protected Health Information: Any Individually identifiable health information that is saved, transmitted or maintained in any electronic form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

Individually Identifiable Health Information: Any Information, including demographic information, collected from an individual that 1) is created or received by a health care provider, health plan, employer, health care clearinghouse, and 2) is related to the past, present, or future physical or mental health or condition of an individual, or the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual which a) identifies the individual, or b) there is reasonable basis to believe that the information can be used to identify the individual.

Privileged information: Information that is protected from seizure and use in court, such as the attorney-client privilege, the peer review privilege, and the like.

Protected Health Information (PHI): Individually identifiable health information that Is transmitted or maintained in any form or medium, by a covered health care provider, or other covered entity, health plan or clearinghouse as defined under HIPAA administration simplification standards.

Request for records: A written document asking the facility to release records to a named entity.

Search warrant: A governmental (court or agency) order authorizing the agency representative to search for and to seize documents or other evidence located in the particular place to be searched.

Sensitive information: Information is considered sensitive if it can be damaging to ERC or its customers' reputation, market standing or a violation of HIPAA.

Subpoena: A court order for ERC to produce records for another facility or person, in this case for a government agency.

Technology Equipment: All computers (desk tops, lap tops, net-books, etc.), printers, copiers, faxes, scanners, USB flash drives, DVD, VCR, cameras, cell phone, telephones, projectors, televisions, cabling, servers, firewalls, spam filters, USB equipment, all routers, cable boxes, voicemail, all software, etc.

Technology Systems: All cell phones, email, Internet, voice mail, telephone, texting, video, web pages, ERC network, files, folders, etc.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

ERC Security Policy Compliance Sign-off Form

I, _____have been trained on the security policies of the Elizabeth Richardson Center, Inc. (ERC). I have had an opportunity to ask questions and receive answers. I understand that these policies are in compliance with the Health Insurance Portability and Accountability Act (HIPAA).

I understand:

- that I am responsible for ensuring the security, integrity and confidentiality of client health information created, obtained and/or maintained by ERC.
- that my job duties require me to use technology equipment and have access to confidential information. Therefore I will comply with all ERC Security policies and procedures.
- that non-compliance will be cause for disciplinary action up to and including dismissal.

I have received a complete set of Security Policies (dated 1/5/2010) and understand that the policies and procedures are available on the ERC network/intranet for my review.

I agree to promptly report all violations or suspected violations of any of the above policies to ERC's Corporate Compliance Officer.

Employee Name (Printed): _____

Employee Signature:_____

Date:_____