Rogue Community Health

Section: Operational Guideline	Approved by: Calisa Warnke, Chief Financial Officer
Number: P-8-OG2	Adopted Date: 12/11/2018
Name: **Sanctions for Privacy and Security Violations**	Sunset Date: 6/30/2021
Number of Pages: 3	Signatures: Calisa Warnke, Terry Koesling

Purpose: Rogue Community Health (RCH) is committed to protecting the confidentiality of all forms of data whether on paper, in electronic form, or discussed verbally. While a commitment to the privacy and security of data is an expectation, there remains a possibility that an inappropriate or unintended access or disclosure of any type of confidential data may result. This operational guideline defines the sanctions for such situations, both willful and unintended.

Parent Policy: P-8 HIPAA

Scope: Applies to all RCH employees, volunteers, temporary staff, students, and contractors.

Definitions:
Confidential Data: Includes, but is not limited to, personally-identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or other harm the individual and/or the organization.

Protected Health Information (PHI): PHI is any information, including demographic information, created or received by a covered entity that relates to:

1. The past, present, or future physical or mental health or condition of an individual
2. The provision of healthcare to an individual
3. The past, present, or future payment for the provision of healthcare to an individual that identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. PHI includes information concerning a person that is living or deceased and may be in written, oral, or electronic format. There are 18 identifiers that the Privacy Rule says can be used to identify a person, including:
    a. Name
    b. All geographic subdivisions of a state, including street address, city, county, and zip code; except for the first three digits in a zip code
    c. All dates directly related to the individual, including birth date, admission date, discharge date, date of death (except for the year)
    d. Telephone number
    e. Fax number
    f. E-mail address
    g. Social Security number
    h. Medical record number (MRN)
    i. Health plan beneficiary number
    j. Account number
    k. Certificate/license number
    l. Vehicle identifiers and serial numbers
    m. Device identifiers and serial numbers
    n. URL address
    o. IP address
    p. Biometric identifiers, including fingerprints

q. Full-face photographs and any comparable images
r. Any unique identifying number, characteristic, or code

4. PHI excludes individually identifiable health information:
   a. In education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended 20 U.S.C. 1232g
   b. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv)
   c. In employment records held by a covered entity in its role as employer
   d. Regarding an individual who has been deceased for more than 50 years

Associated Forms:
Corrective Action for Unauthorized/Improper Access, Disclosure, or Use of Protected Health Information (PHI) & Other Confidential Data

Reference:
CFR 42 § 164.308(a)(1)(ii)(C)

Compliance: Upon discovery of an actual inappropriate or unintended disclosure or access to PHI or confidential data, the Compliance Director will gain approval from the Chief Executive Officer or Chief Operations Officer to make a recommendation for a specified disciplinary action to the appropriate supervisor based on the outlined tiered sanction process. All actual violations or breaches of confidentiality will be reported by the Compliance Director through the Board Policy Committee to the Board of Directors.

Procedure/Workflow/Tasks:

1. All employees, volunteers, temporary staff, students, and contractors that become aware of a potential or actual privacy or security incident are expected to immediately report it through RCH's electronic incident reporting system or by contacting the Compliance Director.

2. The Compliance Director proactively monitors and audits access to RCH systems and facilities.

3. Employees, volunteers, temporary staff, students, and contractors found to have inappropriately accessed or disclosed PHI/ePHI or other confidential data may be subject to the tiered sanctions as described in the Corrective Action for Unauthorized/Improper Access, Disclosure, or Use of Protected Health Information & Other Confidential Data form.

CORRECTIVE ACTION FOR UNAUTHORIZED/IMPROPER ACCESS, DISCLOSURE, OR USE OF PROTECTED HEALTH INFORMATION & OTHER CONFIDENTIAL DATA

Level 1	Level 2	Level 3	Level 4
Accidental *violation due to inadvertent error or lack of proper training.* ***FIRST*** *occurrence of the following:*	***Unintentional*** *violation of privacy or electronic security policies or* ***Repeated*** *number of previous violations.*	***Purposeful*** *violation of privacy or electronic security policies, or an* ***Unacceptable*** *number of previous violations.*	***Purposeful*** *violation of privacy or electronic security policies with associated potential for* ***Patient Harm****.*
☐ Improper disposal of PHI ☐ Unintentionally sending PHI via mail, email or fax to a wrong party ☐ Leaving PHI unattended in a public or common area ☐ Improper handling of medical records or other PHI ☐ Failure to properly sign-off or lock computer when leaving workstation ☐ Failure to properly safeguard username(s) and password(s) ☐ Opening an email attachment from an unknown party that contains a virus, worm, malware or other program that adversely affects RCH's electronic systems ☐ Loss of electronic equipment, keys, swipe cards (badges), or other assigned items that compromise building or PHI security ☐ Other minor violations of established privacy or security procedures. ☐ Other:	☐ Pattern of committing the violations outlined in Level 1 ☐ Release of PHI without proper patient authorization or in accordance with established procedures ☐ Leaving detailed PHI on an answering machine/voicemail w/o permission ☐ Unauthorized installation of electronic hardware or software on RCH equipment and systems ☐ Failure to report privacy and/or security violations in accordance with established procedures ☐ Not accounting for disclosures of PHI as required by established procedures ☐ Not properly verifying patient identity ☐ Failure to properly process a request for confidential communication, restriction on access to PHI, and/or request to amend PHI ☐ Failure to follow established privacy or security procedures ☐ Other:	☐ Unacceptable number of previous violations outlined in Level 1 or 2 ☐ Inappropriately accessing or using PHI, including personal PHI, without having a legitimate job-related reason to do so ☐ Allowing another staff member to access any system or limited access area using personal username or password, key, swipe card (badge) or other security device; improper use of another staff member's personal security information and devices to access any system or enter a limited access area ☐ Transmission of confidential information using an unsecured or unapproved method (i.e., sending unencrypted PHI over the internet) ☐ Willful violation of established privacy or security procedures ☐ Other:	☐ Disclosure of PHI to an unauthorized individual or entity for illegal purposes ☐ Allowing a non-staff member to access any RCH system using personal security information and devices ☐ Any uses or disclosures that could cause harm to a patient ☐ Use of PHI to commit identity theft ☐ Disabling information security tools, bypassing security measures or otherwise compromising electronic security systems ☐ Other:
Recommended Corrective Action: Level 1 Violations ☐ Counseling ☐ Documented retraining on applicable policies and procedures ☐ Other:	**Recommended Corrective Action: Level 2 Violations** ☐ Verbal warning ☐ Documented retraining on applicable policies and procedures ☐ Other:	**Recommended Corrective Action: Level 3 Violations** ☐ Written warning ☐ Documented retraining on applicable policies and procedures ☐ Termination ☐ Other: **Contact HR or RCH Officer prior to termination action**	**Recommended Corrective Action: Level 4 Violations** ☐ Termination ☐ Referral to law enforcement ☐ Other: **Contact HR or RCH Officer prior to termination action**

Notes:

1. It is not possible to address every situation that may involve the inappropriate disclosure or use of PHI. This document lists those violations that occur most commonly and is solely intended to provide general guidance in order to promote a consistent RCH-wide approach to incidents involving the improper use or disclosure of PHI. This document does not limit in any way the discretion of RCH in responding to and taking corrective action related to such matters.
2. RCH reserves the right to make final decisions concerning the interpretation and application of policy or programs. The language used in this guide is for informational purposes only and is not intended to create or constitute a guarantee of employment as employment with RCH is at will.