CATHOLIC COMMUNITY SERVICES
OF WESTERN WASHINGTON

HIPAA SECURITY RULE MANAGEMENT PROGRAM

Policy: HIPAA Security Awareness and Training	**Policy No. HSMP-03**	Reviewed Annually Original Effective Date: 03/14/18
SO Review Completed: 2/2/23	**COG Reviewed**: 06/30/22	**Directors Reviewed**: N/A
COA Date Signed: N/A	*Policy ready to be implemented, effective date of signed COA*	

DESCRIPTION

The CCSWW HIPAA Security Rule Management Program's effectiveness is measured in the performance of CCSWW staff training and implementation of policies and procedures to safeguard the electronic protected health information of individuals enrolled in services. This policy demonstrates CCSWW's commitment to ensure that workforce members are knowledgeable about HIPAA Security Rule requirements and industry best practices. As applicable, CCS security awareness training and educational activities may be conducted to include all forms of Protected Health Information: electronic, paper, and verbal.

POLICY

It is CCSWW policy:

1. 164.308(a)(5) (i): to train workforce members to understand HIPAA Security Rule requirements and related security issues that include, but are not limited to, new threats and security incident reporting.
2. 164.308(a)(5) (ii) (A): to periodically remind CCSWW workforce members of threats to the organization's operational environment and of organizational security best practices.
3. 164.308(a)(5)(ii) (D): to train workforce members to use strong passwords and require, whenever possible, that CCSWW hardware and software platforms enforce strong password parameters. Additionally, CCSWW workforce members are required to change passwords periodically in accordance with the procedures below.
4. That workforce members contact their regional agency's HIPAA Security Officer if they believe additional security training is required in order to perform their job function(s).

PROCEDURE

1. 164.308(a)(5)(i): The HR Department will coordinate with program supervisors to ensure that all regular and contracted employees who work in HIPAA covered entity service areas within CCSWW will receive HIPAA Security training as part of their new hire process and prior to being granted access to the organization's ePHI.

2. The Security Officer Team will ensure that HIPAA security training provides a reasonable and appropriate basis for employees to understand CCSWW's risk tolerance and practices, to include:
    a. Security Rule standards and implementation specifications;
    b. Current local policies and procedures;
    c. Identifying the regional agency/system's HIPAA Security Officer by name;
    d. Threats, alerts and industry best practices; and
    e. Other relevant information technology security topics.

3. The Clinical Oversight Group will create and maintain a HIPAA security test as a training material feedback mechanism. Employees who demonstrate less than an 80% training comprehension will repeat the training and successfully complete the test. The HR Department will document all

training and test scores either in each employee's personnel file or in a consolidated HIPAA Security Program training file.

4. The CCSWW Security Officer Team will evaluate all HIPAA security training as requested and test materials to ensure they enable all employees to fulfill their security responsibilities and that the materials relate to the Security Rule and to local policies and procedures. The Security Officer Team will review the new employee onboarding HIPAA test annually.

5. IT, HR and Data Stewards are responsible to ensure that ePHI access is suspended for those employees unable to demonstrate adequate training comprehension (i.e. until they are able to pass the tests).

6. 164.308(a)(5)(ii)(A): the Security Officer Team will coordinate with designated program managers to provide follow-up training (i.e. HIPAA Security Reminders) as described in paragraph 2 above, at least monthly to all employees who work in CCSWW HIPAA covered entity service areas. Reminders will be delivered as formal training whenever possible, but can include information distributed in email or during meetings. Monthly HIPAA Security Reminders will be retained either in each employee's personnel file or in a consolidated HIPAA Security Program training file.

7. The Security Officer Team will ensure HIPAA security training is an integral part of the culture in all CCSWW HIPAA covered entity service areas (i.e. is not relegated to an annual training requirement).

8. The Security Officer Team will at least once annually, or when asked to do so by the organization's executive leadership, seek workforce member feedback regarding the effectiveness of the security reminders and document the results.

9. 164.308(a)(5)(ii)(D): the CCSWW IT Director, or designee, in coordination with the Security Officer Team, and the HR Department will ensure that security materials will include instructing CCSWW workforce members regarding the creation, changing and safeguarding of strong passwords.

10. The CCSWW Information Technology (IT) Director, or designee, will ensure that password parameters are applied to all hardware and software systems, including mobile devices, as follows:
    a. Passwords use phrases that are unique and difficult to guess but easy to visualize and remember. e.g. #gracefulelEphantdancer$2.
    b. Passwords must be changed every 365 days; may be changed sooner.
    c. Systems will be configured to remember and not allow a password used in the previous six (6) instances.
    d. Systems that employ a personal identification number (PIN) in lieu of a password (e.g. smartphones, etc.) will have their PIN length set to a six-character minimum.
    e. Users are temporarily locked out after 5 unsuccessful attempts to log on.

11. The CCSWW IT Director, or designee, will document and report to the HIPAA Security Officer Team those systems that are technically unable to support the password standards in paragraph 10.

12. The Security Officer Team will document why any of these procedures are not fully implemented, if applicable.