CATHOLIC COMMUNITY SERVICES
OF WESTERN WASHINGTON

HIPAA SECURITY RULE MANAGEMENT PROGRAM

Policy: Workforce Security	**Policy No**. **HSMP-02**	Reviewed Annually Original Effective Date: 06/14/18
SO Review Completed: 07/06/2023	**COG Reviewed**: N/A	**Directors Reviewed**: N/A
COA Date Signed: N/A	*Policy ready to be implemented, effective date of signed COA*	

DESCRIPTION

CCSWW electronic protected health information (ePHI) confidentiality, integrity and availability is protected through administrative safeguards before, during and after workforce member access. Where implementation of specific procedures in this policy may logically include safeguards for paper and verbal forms of Protected Health Information, these forms of PHI are also included.

POLICY

It is CCSWW policy:

1. 164.308(a)(1) (iii) (c): to apply sanctions against workforce members who fail to comply with CCSWW security policies and procedures.

2. 164.308(a)(3)(i) and 164.308(a)(3)(ii)(C): to ensure that workforce members have appropriate access to ePHI and to prevent unauthorized access to ePHI by all workforce members. E-PHI access will be terminated when workforce member employment ends or as required.

3. 164.308(a)(3)(ii) (A): that supervisors will authorize workforce member ePHI access and will supervise the ePHI access with reasonable and appropriate safeguards.

4. 164.308(a)(3)(ii)(B): to ensure that prospective workforce members are screened to ensure that credentials are authentic and current, and to ensure that no unreasonable risk to ePHI is introduced, prior to being granted ePHI access.

5. Provisions of this policy regarding unauthorized workforce member access to or disclosure of protected health information shall apply to all forms of such information, including verbal, paper and electronic.

PROCEDURE

1. 164.308(a)(1)(ii)(c): The Human Resources Department will apply tiered workforce member sanctions. The sanctions apply to unauthorized workforce member PHI access or disclosure and not to the authorized access required to support CCSWW client safety.
    a. Accidental unauthorized PHI access or disclosure will result in the workforce member receiving a written letter of instruction from their supervisor that documents the incident and training actions, to ensure that the workforce member understands how to prevent reoccurrence. The supervisor will forward a copy of the letter to the Human Resources Department. In the case of more than one accidental disclosure within a 12 month period, CCSWW will determine whether the workforce member's performance pattern meets careless unauthorized PHI access or disclosure criteria.
    b. Careless unauthorized PHI access or disclosure will result in the workforce member receiving a written letter of instruction from their supervisor that documents the

incident and training actions to ensure that the workforce member understands how to prevent reoccurrence. The supervisor will forward a copy of the letter to the Human Resources Director. Additionally, the workforce member will be placed on a Corrective Action Plan per CCSWW Human Resources policies or the CCSWW-Northwest Collective Bargaining Agreement, as applicable. In the case of more than one careless unauthorized access or disclosures within a 12 month period, CCSWW will determine whether the workforce member's performance pattern meets deliberate unauthorized PHI access or disclosure criteria.

c. Deliberate unauthorized PHI access or disclosure will result in the workforce member's immediate termination.

The Human Resources Department will report all unauthorized PHI access or disclosure to the HIPAA Security Officer and the HIPAA Privacy Officer in the region where the violation occurred, or vice versa, depending on which party is first aware of the unauthorized access or disclosure.

2. During the new hire orientation process, the Human Resources Department will inform newly hired employees of the *Acknowledgment of Responsibilities* form which discusses the importance of safeguarding CCSWW PHI. This form will be forwarded on to the employee's assigned program supervisor for detailed discussion of its contents, including policy on tiered sanctions for unauthorized PHI access or disclosure, whether accidental, careless or deliberate. All workforce members will sign the acknowledgment before being granted access to CCSWW PHI and supervisors will return the form to HR for filing in the employee's personnel file.

3. 164.308(a)(3)(i): Working with data owners, program managers and HR as necessary, data stewards will create and maintain a formal process (e.g. a spreadsheet) to ensure appropriate workforce member ePHI access or change.

4. Data stewards and data owners will ensure security groups are created for all systems to ensure that workforce members have appropriate access to perform their duties, and share this information with program managers and HR as necessary for inclusion in the process described in paragraph 3.

5. Data owners and data stewards will identify security groups for electronic systems (e.g. EMR) that access ePHI to ensure that workforce members have appropriate access to perform their duties, relative to each system's risk. No device will have access to ePHI that creates a high level risk.

6. The IT Director, or designee, will ensure that executive workforce member access is appropriate to the corresponding job function and report to the CCSWW Executive Vice President - Chief of Operations those cases where an executive workforce member persists to either request or direct ePHI access not integral to their position.

7. Data owners will retain all CCSWW network ePHI system access, modification and termination requests for six years.

8. IT system administrators/data stewards/data owners will verify all accounts belonging to workforce members:
    a. quarterly in the primary electronic health record system;
    b. quarterly in the Active Directory and network access (e.g. VPN, etc.) systems; and
    c. semi-annually for all other systems.

9. 164.308(a)(3)(ii)(A): Regional Agency and/or System Directors will maintain CCSWW's organizational charts to communicate a clear workforce member relationship.

10. The Human Resources Department will ensure all position descriptions reflect ePHI safeguard responsibilities. The HR Department will include supervisor position description responsibilities to approve and monitor subordinate ePHI system access.

11. Data stewards will use the process in paragraph 3 to establish or modify workforce member ePHI access. Only supervisor requested access to systems will be granted.

12. 164.308(a)(3)(ii(B): As required by CCSWW Human Resources policies and any additional requirements required by specific program contracts, the Human Resources Department will conduct background checks on all prospective employees, including those whose duties allow access to protected health information (all forms).

13. The Human Resources Department will ensure each employee signs a confidentiality agreement prior to accessing CCSWW protected health information (all forms).

14. The Human Resources Department will ensure that a confidentiality agreement is kept current (signed annually) and relevant.

15. Supervisors will ensure their staff has the necessary knowledge and skills to use and safeguard CCSWW information systems, commensurate with their access to ePHI.

16. 164.308(a)(3)(ii)(C): Program directors in HIPAA covered entity service areas will define and maintain a formal process (e.g. a single printed or electronic form) to request workforce member ePHI systems termination under routine circumstances in which employees leave the organization or covered entity program. Circumstances that involve expedited workforce member separation will originate from the HR Department. HR will take necessary steps to ensure expedited termination of the separating workforce member from ePHI systems, including notification of IT and data owners who need to know such circumstances The HR Department will notify the HIPAA Security Officer in any instance that ePHI access is removed for reasons other than routine employee termination or reassignment.

17. The HR Department will verify and report to the IT Department and to the Data Steward any requested closure of workforce member ePHI information system access.

18. The IT Department and the HR Department will ensure workforce member termination is performed as detailed in the process and ensure involuntary termination access is performed in a timely manner that does not risk the confidentiality, integrity or availability of CCSWW ePHI.

19. Program Directors will ensure there is a process in place (e.g. a checklist) for all covered entity sites to account for retrieval or disabling of all workforce member security devices (e.g. keys, identification badges, computer login credentials, portable computing devices, etc.) as part of the employee termination process.

20. Supervisors will use the process in paragraph 16 to terminate workforce member ePHI access. When not practical to use the process prior to terminating ePHI access, the Human Resources Director or HIPAA Security Officer will request workforce member access termination and the supervisor will follow the process to create an audit trail.

21. The HIPAA Security Officer will document in the Security Log why any of these procedures are not fully implemented, if applicable.