CATHOLIC COMMUNITY SERVICES
SERVING PEOPLE OF ALL BELIEFS

HIPAA SECURITY RULE MANAGEMENT PROGRAM

Policy: Business Associates	**Policy No. HSMP-09**	Reviewed Annually Original Effective Date: 11/14/18
SO Review Completed: 05/04/2023	**COG Reviewed**: N/A	**Directors Reviewed**: N/A
COA Date Signed: N/A	*Policy ready to be implemented, effective date of signed COA*	

DESCRIPTION

The CCSWW HIPAA Security Program is designed around policies and processes to properly safeguard electronic protected health information (ePHI) from unauthorized disclosure as is reasonable and appropriate to the organization.

POLICY

It is CCSWW policy:

1. 164.308(b)(1), 164.314(a)(1) and 164.314(a)(2)(i): to, via a signed contract, permit third parties (Business Associate) to create, receive, maintain or transmit ePHI only after the Business Associate provides satisfactory assurances that it fully complies with the HIPAA Security Rule and appropriate safeguards CCSWW's ePHI.

2. 164.308(b)(2) and 164.314(a)(2)(i): to allow its Business Associates to subcontract functions on their behalf that create, receive, maintain or transmit ePHI. CCSWW will ensure that the Business Associate obtains satisfactory assurances that the subcontractor Business Associate fully complies with the HIPAA Security Rule and appropriately safeguards CCSWW's ePHI.

3. 164.308(b)(3): that any written Business Associate contract complies with these referenced Security Rule standards and implementation specifications.

4. 164.314.(a)(2)(i): to ensure the Business Associate or subcontracted Business Associate reports to CCSWW any security incident of which either becomes aware, including breaches of unsecured protected health information.

PROCEDURE

1. *All policy references apply*: CCSWW HIPAA Security Officers will ensure no CCSWW ePHI is accessed by a Business Associate until a contract is signed between CCSWW and the affected Business Associate.

2. CCSWW HIPAA Security Officers will perform reasonable and appropriate due diligence that attests to the Business Associate's ability to adequately safeguard CCSWW's ePHI (e.g. review the Business Associate's security risk analysis, etc.) prior to signing the Business Associate contract.

3. CCSWW HIPAA Security Officers will ensure each Business Associate contract is binding, compliant with state laws, and is unique to the relationship with the Business Associate, and incorporates:
    a. Explicit permitted and required uses of ePHI;
    b. All applicable Privacy Rule standards and implementation specifications;
    c. Security requirements to address the confidentiality, integrity and availability of CCSWW ePHI;
    d. The requirement for the Business Associate to completely comply with the Security Rule and Breach Notification Rule;
    e. The requirement for the Business Associate to report to CCSWW any security incident of which it becomes aware, including breaches of unsecured protected health information as required by 164.410;

f. The requirement for the Business Associate to execute a Security Rule compliant contract with any subcontractor prior to providing access to CCSWW ePHI;
g. The requirement for the Business Associate to obtain satisfactory assurances that the subcontractor will appropriately safeguard CCSWW ePHI;
h. The requirement for the Business Associate to ensure that the subcontractor will comply with the HIPAA Security and Breach Notification Rules; and
i. Provisions for terminating the agreement, including the Business Associate's return or disposal of CCSWW's ePHI, when feasible.

4. CCSWW HIPAA Security Officers will ensure the regional organization's BAA list is current and each Business Associate contract is reviewed for accuracy no less than annually. Annual BAA list reviews may correspond with annual review of HSMP 09 and be reported on at SO meeting.