CATHOLIC COMMUNITY SERVICES
SERVING PEOPLE OF ALL BELIEFS

HIPAA SECURITY RULE MANAGEMENT PROGRAM

Policy: e-PHI Availability	**Policy No. HSMP-08**	Reviewed Annually Original Effective Date: 11/14/18
SO Review Completed: 09/07/2023	**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 will incorporate procedures for protecting and responding to an emergency that affects the availability of electronic protected health information (ePHI).

POLICY

It is CCSWW policy:

1. 164.308(a)(7)(i): to implement a contingency plan to respond to emergencies or other occurrences (e.g. fire, vandalism, system failure, natural disaster) that damage ePHI services.

2. 164.308(a)(7((ii)(A): implement a backup plan that creates and maintains retrievable exact copies of ePHI.

3. 164.308(a)(7)(ii)(B): implement a disaster recovery plan capable of restoring any loss of data.

4. 164.308(a)(7)(ii)(C): continue critical business processes for protecting ePHI security while operations continue in emergency mode.

5. 164.308(a)(7)(ii)(D): periodically test and revise contingency plans.

6. 164.308(a)(7)(ii)(E): understand the relative criticality of specific applications and data in support of contingency plan operations.

PROCEDURE

1. 164.308(a)(7)(i): CCSWW covered entity site data owners, along with IT, will identify all ePHI critical applications, data, operations and processes and ensure they are accounted for throughout this procedure.

2. With input from covered entity site directors and IT, Security Officers will identify reasonable and appropriate contingency plan preventative measures for the covered entity sites in their respective regions. Contingency Plans (aka Business Continuity Contingency Plans or BCCPs) address four elements: a) criticality analysis; b) emergency mode operations plan; c) disaster recovery plan; d) data back-up plan.

3. Security Officers will define ePHI objectives within CCSWW's overall contingency planning. Each CE program will maintain Contingency Plans that contain site-specific details, using the *CCSWW Business Continuity Contingency Plan (BCCP)* form. This form provides for documentation of all elements of this policy related to contingency planning.

4. The HIPAA Security Officer Team will ensure that contingency planning includes objectives, framework, roles and responsibilities. These elements will be included in each CE site's document – *CCSWW Business Continuity Contingency Plan*.

5. The HIPAA Security Officer will review the process used to identify critical ePHI applications, data, operations and processes, to ensure they support contingency planning performance criteria.

6. 164.308(a) (7)(ii)(A): the IT Department and system owners will ensure all ePHI is backed up, based on service criticality and the frequency that new information is introduced. For EMR applications that are not backed up by CCSWW servers, Regional Security Officers will maintain documentation provided by EMR vendors that details how data is backed up, including frequency, scope, backup method and backup media location that accounts for protecting ePHI in the event of a disaster that impacts data on EMR vendor servers

7. The IT Department will document backup frequency and scope, backup method, and backup media location that accounts for protecting ePHI in the event of an onsite disaster impacting CCS held data.

8. The IT Department will ensure that backup performance is monitored through log review or other methods.

9. The IT Department will ensure that backup media is encrypted.

10. The IT Department will randomly test backup media quarterly with partial data restores to a test environment service host, not to interfere with live services, and document the results (e.g. time to restore, data integrity, etc.).

11. The IT Department will report to the Regional HIPAA Security Officer any failed ePHI service backup attempt or any failed ePHI service restore test, and a documented root cause analysis that includes a solution to the failure(s).

12. 164.308(a)(7)(ii)(B): The IT Department will create a disaster recovery plan as part of the Business Continuity Contingency Plan (BCCP)to restore service functionality and exact copies in the event of an emergency.

13. CE site Program Directors, IT, and the Regional SO will analyze and implement as resources allow, alternative-site solutions that account for when the primary data center is not available (e.g. fire damage, etc.).

14. The IT Department will provide communication and access procedures for live ePHI stored offsite (e.g. cloud vendors, etc.).

15. The IT Department and system owners will train and evaluate the workforce members' ability to successfully implement the disaster recovery plan.

16. The HIPAA Security Officer will review regional Business Continuity Contingency Plans no less than annually.

17. 164.308(a)(7)(ii)(C): The IT Department will provide details to continue critical ePHI services and protect ePHI security, when the contingency event is more limited and does not require the disaster recovery plan (e.g. one ePHI service casualty), into CCSWW's emergency operations mode plan.

18. The HIPAA Security Officer will review the emergency operations mode plan and its associated risk with assistance from the IT Department no less than annually.

19. 164.308(a)(7)(ii)(D): The HIPAA Security Officer will coordinate annual contingency plan testing that varies emergency scenarios and requires both the disaster recovery plan and the emergency mode operations plan.

20. The HIPAA Security Officer will ensure that lessons learned from testing are incorporated into all contingency planning documents and ensure the contingency planning remains reasonable and appropriate, relative to CCSWW's resources.

21. 164.308(a)(7)(ii)(E): Using the information collected from paragraphs 1 and 3, the IT Department will analyze and prioritize service restoration in support of contingency plan operations.

22. The HIPAA Security Officer will review the service restoration analysis with the IT Director no less than annually.

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