CareNu		Effective Date:	11/10/2023
Policy Title:	Confidentiality of Information	Last Review Date:	03/15/2024
Issuing Department:	Systems	Last Revision Date:	11/10/2023
Policy Number:	HE.02.07	Next Review Date:	03/15/2025
Applies to:	☐ ACO ☐ MSO ☐ TPA ☒ ALL		

Policy

It is the Policy of the above Organization(s) to maintain the confidentiality of all protected health information (PHI) including medical, financial, and personal information belonging to patients. Confidentiality pertains to all information in verbal, paper or electronic format and includes, but is not limited to; diagnosis, type of treatment, patient response to treatment, psychosocial notes, claims information, photographs or any written documents containing social security, or tax identification.

Purpose

To ensure that the patient's right to privacy is protected by following the policies and procedures regarding confidentiality and use and disclosure of protected health information (PHI), as necessary.

Scope

This process applies across the organization.

Definitions

N/A

Procedure

To ensure the privacy and security of confidential information, the following shall be followed:

1. All employees, volunteers, students, and contractors will complete HIPAA awareness training. Everyone will review and sign the Confidentiality and Security Agreement prior to start of any duties.

2. Authorization (verbal, electronic or written) must be obtained prior to discussing information involving a patient. Review the verbal release of information to verify appropriate authorization. Any verbal authorizations must be documented in the patient medical record utilizing the verbal consent.

3. Comments and conversations relating to patients made by physicians, nurses, or other hospice personnel will be made in confidential settings. It will be standard, acceptable, and necessary practice to share information with other members of the care team. The decision to share information can be aided by considering the intent of the discussion.

4. Protected Health Information (PHI) is not to be discussed with others who do not have a need to know the information.

5. PHI is not to be stored on personal devices, such as cell phones, tablets, laptops, cameras, or any other non-owned agency device. No exceptions.

6. Use and disclosure of PHI will be carried out according to accepted policies and procedures.

7. Only the information needed to do your job shall be accessed or obtained. Employees and volunteers are not allowed to access their own medical or financial records or those of family members, friends, coworkers, neighbors, or high-profile individuals.

8. When traveling with mobile devices (i.e. laptop, tablet, cell phone), ensure the device is secure in the trunk of your car. Devices should not be left in vehicles for extended periods of time to protect them from damage due to extreme heat or cold.

9. Privacy covers are to be utilized for clipboards that are used to document patient information.

10. Privacy screens are to be utilized for monitors that are in areas accessible by the public.

11. Records at nursing stations must be stored in a secure manner to prevent unauthorized visualization of patient information.

12. When leaving workstation unattended, lock the computer or log off the workstation.

13. Login Information must be always protected. Never allow anyone to utilize your Login Information.

14. Never send protected health information in an e-mail to a location outside of the organization. Any protected health information that must be sent to an outside agency must be coordinated with the CIT department.

15. Texting of PHI is not allowed, as this is an unsecured method of communication. Texting PHI must be done using a secured texting application (not your devices native SMMS application). Please contact the IT Department (CIT) if you have questions regarding which secure messaging solution is approved and available for use. Secure Messaging PHI to anyone outside of the organization that is not involved in the patient's care, including but not limited to, healthcare provider, insurance company, SNF/ALF, DME, or Pharmacy, is strictly prohibited. If you have questions regarding the sharing of information, you should consult with Compliance or the IT Department (CIT).

16. Requests for copies of medical records must be forwarded to the Compliance or Health Information Management (HIM) Department for processing. NO EXCEPTIONS!

17. All documents with patient identifiable information must be disposed of in a secure manner. Any confidential documents must be placed in designated secure shred bins for appropriate disposal.

18. Any electronic media containing PHI will be followed by the Information Technology policy for appropriate disposal.

19. Violations of this policy may result in disciplinary action, up to and including termination.

References

HE2 Element F Factor 1-3 Privacy protection for data.

Approval/Revision History

Version Number	Change Date; (Original/ Reviewed/ Revised)	First Level Approval	Second Level Approval
V1	11/10/2023 Original	Name: Matthew Strohhacker Title: Sr. Director, Systems 11/10/2023 Date	Name: Maya Kaczmarek Title: Sr. Director, Operations 11/10/2023 Date
V1	03/15/2024 Reviewed	Name: Matthew Strohhacker Title: Sr. Director, Systems 03/15/2024 Date	Name: Maya Kaczmarek Title: Sr. Director, Operations 03/15/2024 Date