CareNu		Effective Date:	11/10/2023
Policy Title:	HIPAA Privacy - Access, Authorization, Use, and Disclosure of Protected Health Information	Last Review Date:	03/15/2024
Issuing Department:	Systems	Last Revision Date:	11/10/2023
Policy Number:	HE.02.09	Next Review Date:	03/15/2025
Applies to:	☐ ACO ☐ MSO ☐ TPA ☒ ALL		

Policy

It is the policy of the Organization to fully comply with the Health Insurance Portability and Accountability Act of 1996 (the "Act") and the rules promulgated thereunder (the "Rules"), as such Act and Rules may be amended or supplemented from time to time (collectively, "HIPAA"). Accordingly, in furtherance of this policy and when applicable to an Organization's actions, either as (a) a covered entity (b) a business associate of such affiliated covered entity, such Organization(s) shall comply with the requirements set forth below regarding access to, use of and disclosure of Protected Health Information (PHI).

Purpose

To ensure proper protection and compliance with the Health Insurance Portability and Accountability Act of 1996.

Scope

This process applies across the organization.

Definitions

Business Associate: A person or entity that, on behalf of a Covered Entity, creates, receives, maintains, or transmits protected health information for claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and re-pricing; or that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity, where the provision of the service involves the disclosure of protected health information from such Covered Entity, or from another Business Associate of such Covered Entity, to such person or entity.

Covered Entity: A health care provider that transmits or maintains Protected Health Information in oral, electronic, written, or any other form. Health plans and health care clearinghouses are also considered covered entities under HIPAA.

Protected Health Information: Any information, whether oral or recorded in any form or medium, that is (a)

created or received by a health care provider and (b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past,

present, or future payment for the provision of health care to an individual, and (c) either identifies or could be used to identify the individual.

Procedure

1. The Organization requires and informs individuals that requests for access to Protected Health Information must be made in writing.

2. The Organization uses an authorization form that meets the requirements of State and Federal regulations.

3. A valid authorization for release of protected health information (PHI) must contain the following core elements and required statements to be considered valid:

    a. Core Elements

        i. Name of the individual or institution authorized to release the information.
        ii. Name of individual or institution that is to receive the information.
        iii. Patient's full name and date of birth
        iv. A description of the purpose or need for the information.
        v. Description of information to be used or disclosed.
        vi. Specific date, event or condition upon which consent will expire or be revoked.
        vii. Date the authorization is signed.
        viii. Signature of patient or legal representative and description of authority.

    b. Required Statements

        i. The individual's right to revoke the authorization in writing, the exceptions to the right to revoke and a description of how the individual may evoke the authorization.
        ii. The authorization may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization.
        iii. The potential for the information disclosed pursuant to the authorization to be subject to re-disclosure by the recipient and no longer protected by HIPAA.

4. The Organization is not required to obtain an authorization from the patient to use or disclose protected health information for:

    a. treatment, payment and health care operations;
    b. treatment activities of another health care provider;
    c. payment activities of the entity to which PHI is disclosed; and
    d. health care operations of another covered entity if:

i. both the organization and the other covered entity has or has had a relationship with the individual and the PHI involved pertains to that relationship; and/or
ii. the disclosure is for specified health care operations purposes (including quality assessment and improvement activities, case management or care coordination, training, accreditation or licensing activities) or fraud and abuse detection or compliance.

5. When authorization is needed, the patient or his or her legal representative is provided with a copy of the authorization form and asked to sign it.

6. Signing the authorization form is voluntary and the patient or his or her legal representative may refuse to sign it.

7. The authorization may be revoked (in writing) by the patient/legal representative at any time.

8. The permissions granted in the authorization may <u>not</u> be acted upon if it has been revoked or if it has expired.

9. The authorization is documented and retained for a period of seven (7) years after it was created or expired, whichever date is later.

10. When a request for access to Protected Health Information is received, it will be acted upon within thirty (30) days from the date of the request.

11. The time frame stated above may be extended one time for no more than thirty (30) days if the requested information is maintained offsite. If the extension is necessary, the Organization will provide the individual with a written statement that specifies the reason(s) for the delay and the date by which the individual may expect to receive access to the Protected Health Information for inspection or to obtain a copy.

12. The Organization maintains the designated records, in which the Protected Health Information that may be subject to requests for access is contained, for a minimum period of seven years and maximum of 10 years, from the date it was created or was last in effect, whichever is later.

13. The Organization maintains the titles of the persons/offices responsible for receiving and processing requests for access to Protected Health Information for a minimum period of seven years and maximum of 10 years, or for pediatric patients seven years after they turn eighteen (or would have turned eighteen).

14. With respect to deceased patients of each Organization that operate as a hospice in Florida:

    a. A deceased person's hospice records cannot be released in response to a subpoena, even if such subpoena complies with all applicable requirements of HIPAA, without proper legal documents:

i. Will designating requestor as representative or executive of will,
ii. Letter of Administration on behalf of deceased from a court, or
iii. A court order from a competent jurisdiction.

b. If the requestor is listed on the patient's *Hospice Election and Consent* form in the Authorization for Release of Information section, records may be released.

c. Instances in which State law requires or authorizes the release of the hospice records of deceased persons in the absence of a court order include, but are not necessarily limited to disclosures:
   i. to medical examiners,
   ii. for research certain purposes, and
   iii. to state investigators in connections abuse, neglect and exploitation investigations.

d. Absent a required legal document noted above (a), or the requestor being on the patient's election and consent form (b), no hospice record of a deceased hospice patient is released without the approval of the Compliance Department of CareNu, Inc.

e. In addition to complying with all applicable HIPAA requirements concerning PHI of deceased persons, each Organization will comply with the applicable State laws concerning the confidentiality of health information of the Protected Health Information of a deceased individual for a period of 50 years following the death of the individual.

f. To ensure appropriate release of information guidelines are followed at all times, the person responsible for the management of the medical records at an Organization will consult with the Compliance Department of CareNu, Inc., on an as needed basis, regarding release of information requests related to deceased patients.

g. A Covered Entity must maintain the privacy of the Protected Health Information of a deceased individual for a period of 50 years following the death of the individual.

RELEASE OF PROTECTED HEALTH INFORMATION TO PATIENT/OUTSIDE ENTITY

1. PHI pertaining to a patient and/or family member will not be released to an outside entity without the approval of the Director of Information Systems/designee. The Director will confer with the Privacy Officer and/or Compliance Department in cases that are questionable prior to release of any information.

2. General Guidelines for Release of Information

   a. Information of a confidential nature must not be disclosed by the organization except as

permitted in this policy.

b. The organization will not voluntarily use a medical record in any manner in which it will jeopardize the interests of the patient, with the exception for use of the record, if necessary, to defend itself or its agents.

c. Only the minimum amount of information necessary should be released in response to a valid request.

d. Patients and/or their legal representative may obtain confidential information after a valid authorization to release medical information has been received.

e. Requests for information will be in writing and referred to the Director of Information Systems or designee(s) for the organization. The Director shall review the request and consult with the Privacy Officer and Compliance

   Department as necessary.

f. Information Systems Lead Processor(s) or designee(s) will enter a HIPAA Disclosure in the Client Chart for an accurate accounting of disclosures as required by regulation. The original consent form is retained in the record.
g. If the patient is a minor, the authorization must be signed by a parent or legal representative. In certain instances when the patient is an emancipated minor, he/she may sign his/her own authorization.
h. If the patient is deceased, proper legal document(s) are required to release information in absence of a valid authorization.
i. In the event the patient is unable to sign the authorization by reason of physical or mental disability, the authorization should be signed by the legal representative and the reason why the patient is unable to sign should be documented.

j. Physicians may obtain medical records if they are involved in the care of a patient in the care program.

k. In no instance are copies of medical records to be made without the specific approval of the Director of Information Systems, who will confer with the Director of Compliance/Risk and/or Privacy Officer.
l. All or portions of a medical record may be provided to the organization's Privacy Officer or Chief Compliance Officer to protect the interests of the organization in cases involving liability or compensation.
m. The organization will not charge for medical records unless excessive time is needed to produce the records.
n. Information may be released to third party payers upon verification of the insurance company and provided the patient and/or legal representative has signed the *Hospice Election and Informed Consent* or the Home Health, Palliative Care *Patient Agreement and Informed Consent for Care (PAICC)* form.
o. In all cases, prior to releasing protected health information, check the patient's medical record for HIPAA Restrictions form for limitations that may have been stipulated by the patient and/or legal representative.
p. When an Organization cannot honor a request for the release of protected health information because such request (i) is not made in writing or (ii) is otherwise invalid (e.g. the requestor has

no authority to act on behalf of patient, the authorization submitted with the request is not HIPAA compliant, or the patient is deceased and the request was not accompanied by a court order, etc.), then the Organization shall notify the requestor within 10 business days of receipt of the request.

q. Home health record requests from the patient shall be processed and provided to the patient free of charge, with appropriate release and request, at the next home visit or within 4 business days of the request (whichever comes first).
r. In response to a valid verbal request, the Organization shall provide the requestor with an *Authorization for Release of Information* form and ask that the requestor complete and submit such form.

3. Emergency Conditions

When information has been released in the best interest of the patient under emergency conditions and an authorization to release information could not be obtained due to incapacity or emergency, the staff member responsible for the release of information shall document pertinent details in the medical record Disclosure Release form including the following information at the minimum:

a. The date the information was released.
b. The person to whom the information was released.
c. The reason the information was released.
d. The reason the consent could not be obtained.
e. Details specific to the information released.

4. Exceptions (Authorization Not Required)
    a. CareNu Quality Improvement activities.
    b. Information needed for continuity of care released to another health facility or physician.
    c. For public health activities.
    d. Official surveys for compliance with accreditation, regulatory, and licensing agencies.
    e. Information released to authorized representatives of Florida State agencies in accordance with mandatory reporting requirements (i.e., Adult Protective Services, Dept. of Children & Families).
    f. The Medical Examiner, pursuant to Florida statute.
    g. In compliance with a court order.
    h. Law enforcement officials or activities (see Disclosures for Law Enforcement Purposes section).
    i. Department of Professional Regulation for the investigation of a licensed physician or healthcare worker pursuant to Florida statute.
    j. Funeral homes with a need for pertinent information relative to the filing of a death certificate.
    k. Organ procurement organizations if the patient has indicated they are an organ donor in the medical record.
    l. Emergency preparedness personnel.
    m. Military and veteran activities.
    n. CareNu Institutional Review Board approved research activities.

5. AIDS/HIV Records
    a. Records containing AIDS/HIV information will not be faxed unless an urgent medical need is identified.
    b. Prior to releasing information, check to verify that an authorization, specific for the release of AIDS/HIV information is present, signed and dated.

6. In the absence of the appropriate authorization, an Authorization to Release Medical Information is sent to the patient's place of residence to obtain the signature of the patient (or legal representative).

7. Psychiatric Cases/Psychosocial Counseling Notes
    a. It is policy of the organization to treat all psychiatric cases, psychosocial assessments, counseling notes, alcohol and drug records as super confidential to protect the rights and confidentiality of the patient.
    b. The Director of Information Systems will confer with the Privacy Officer and/or Compliance Department in cases that are questionable.
    c. Super confidential information will only be released with an appropriate authorization issued by the patient/family or court order.

8. Disclosures for Law Enforcement Purposes (without authorization)
    Subject to verification of identity and authority of the law enforcement official, disclosures

    are permitted as follows:

    a. To comply with a court order.

    b. To respond to an administrative request or investigative demand. The request should include a statement that the information requested is relevant and material, specific and limited in scope and a statement stating that de-identified information cannot be used.

    c. To respond to a verbal or written request for PHI for purposes of identifying or locating a suspect, fugitive, material witness or missing person. Disclosures must be limited to:
        i. Name and address
        ii. Date and place of birth
        iii. Social security number
        iv. ABO blood type and *rh* factor
        v. Type of injury
        vi. Dates of service
        vii. Date and time of death
        viii. Distinguishing physical characteristics

    d. To alert law enforcement to the death of an individual when there is suspicion that the death resulted from criminal conduct.

    e. To report PHI the organization believes to be evidence of a crime that occurred on premises of the organization.

    f. To federal officials authorized to conduct intelligence, counter-intelligence and other national security activities.

g. To respond to a request for PHI by a correctional institution or law enforcement official having lawful custody of an inmate if they represent that PHI is needed to provide health care to the individual, for the health and safety of the individual, other inmates, or employees of the correctional institution.

9. Denial of Access

a. The organization may deny a patient's access to their information only in the following Circumstances (These are unreviewable grounds for denial):
    i. During the course of research involving treatment, provided if the patient has agreed to the temporary suspension of access when consenting to participate in the study. The patient's right to access the information will be reinstated upon completion of the research.
    ii. The information in question was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information. The Director of Information Systems will inform the patient where to direct their request, if known.

b. Access may also be denied in the following circumstances; however, the patient must be given the right to have such denials reviewed.
    i. A licensed health care professional has determined that access to the patient's medical information is likely to endanger the life or physical safety of the patient or another person.
    ii. The information requested makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined access to the information is likely to cause substantial harm to the other person.
    iii. The request for access is made by the patient's legal representative and a licensed health care professional determines that the provision of access to the legal representative is likely to cause harm to the patient or another person.

10. Denial Review

a. If a patient requests a review of the denial, the Director of Information Systems will contact the Privacy Officer and/or corporate Director of Compliance, Risk to promptly designate a licensed health care professional, who was not directly involved in the denial process, to review the decision to deny access.
b. The reviewer must determine, within a reasonable period of time, whether or not to deny access to the information requested.
c. A written notice of determination must be promptly provided to the patient.
d. The organization will take the appropriate action to carry out the final determination of the designated reviewer.

11. Information Systems Department Process for Requests

a. Social Security Disability (SSD) Requests
    i. After the request is received, ensure a valid authorization is present.
    ii. The Information Systems Processor shall print then fax the Medical Staff History & Physical (H&P), CL Summary, Initial and Comprehensive Assessment, Medical Staff Clinical Note, and Discharge Summary and Checklist to the fax number listed on the letter.
    iii. The HIM Processor shall enter a HIPAA Disclosure form in the appropriate area of the EMR i.e., Solutions/Forms

b. Attorney Requests/Subpoenas/ Court Orders Requests (Active or Discharged Alive)
    i. **All subpoenas shall only be accepted at the CareNu Home Office**.
    ii. Compliance Department will send a record of the request to Information System Lead Processor.
    iii. The Information Systems Processor shall ensure a valid authorization is signed by the patient.
    iv. If there is not a signed authorization by the patient, the Information Systems Processor shall request documentation of Legal Representative- Durable Power of Attorney, Healthcare Surrogate
    v. Once all verification of the necessary authorization is complete, the Information Systems Processor shall copy only the requested information and put it in the appropriate order for records. Information Systems will place the record in the shared Compliance Information Systems directory, and will email the CareNu Compliance Group email distribution group it is there.
    vi. The Compliance Department will process the final release of records when all authorizations are reviewed to meet the requirements under the Florida Statutes and HIPAA as appropriate.
    vii. The Compliance Department shall send the request and the copied medical record information to the designated person requesting it, and notify Information Systems that the record has been sent.
    viii. The Information Systems Processor shall enter a HIPAA Disclosure in the appropriate area of the EMR i.e., Solutions/Forms once the Compliance Department has released the records to the requester.

c. Insurance Company Requests (Active or Live Discharges)
    i. After the request has been received, the Information Systems Processor shall verify the patient status (active or deceased) in the EMR.
    ii. For active patients, the Information Systems rocessor shall ensure a valid authorization is signed by the patient
    iii. If there is not a signed authorization by the patient, the Information Systems Processor shall request documentation of Legal Representative- Durable Power of Attorney, Healthcare Surrogate.
    iv. Once all verification of the necessary authorization is complete, the Information System Processor shall copy only the requested information and put it in the appropriate order for records. Information Systems will place the record in the shared Compliance HIM directory, and will email the CareNu Compliance Group email distribution group it is there.

v. The Compliance Department shall send the request and the copied medical record information to the designated person requesting it and notify Information Systems the record was sent.
vi. The Information Systems Processor shall enter a HIPAA Disclosure in the appropriate area of the EMR i.e., Solutions/Forms once the Compliance Department has released the records to the requester.

d. Deceased Patient Information Requests

The Information Systems Processor shall send requests to the home office Compliance Department for review. The Compliance Department designee shall ensure:

i. At least one of the following legal documents are present to release the records:
    1) A will showing requestor as executor of the will or as representative.
    2) Court issued *Letters of Administration* that must be signed by a judge. The *Letters of Administration* will indicate who the appointed requestor (personal representative) of the deceased patient.
        a) A court order must be signed by judge, entered by a court of competent jurisdiction requiring the release of hospice records.
ii. Once all verification of the necessary authorization is complete Compliance will notify HIM to process the record.
iii. The Information Systems Processor shall copy only the requested information and put it in the appropriate order for records. HIM will place the record in the shared Compliance Information Systems directory, and will email the CareNu Compliance Group email distribution group it is there.
iv. The Compliance Department shall be responsible for sending all records and notifying Information System when the records are sent.
v. The Information Systems Processor shall enter a HIPAA Disclosure in the appropriate area of the EMR once the Compliance Department has released the records to the requester.

e. Patients/Family members of <u>active</u> patients Requests

i. The patient or family member must complete a Release of Information Authorization form.
ii. For requestors (family member) who are not the patient, the requestor (family member) must be a Healthcare proxy, Power of Attorney or Legal Representative.
iii. The Information Systems Processor shall ensure the requestor (family member) is authorized as the patient contact.
iv. If the requestor is not the authorized patient contact, escalate to the Corporate Health Information Supervisor.
v. After the verification process is complete, the Information Systems Processor shall send the requestor a self-addressed stamped envelope with instruction to the requestor to complete then return the Release of Information Authorization form to the Information Systems department.

f. The following are important to remember when processing Release of Information requests:

i. For anyone picking up medical records, obtain a copy of their photo ID
ii. For SSD requests, the Social Security Administration will automatically send a check for the cost of copies. The check amount is $14.00.
iii. Release of information for medical records are given to the following without a patient authorization:
    1) Medical Examiner Office
    2) Department of Children and Family (DCF)
    3) Law Enforcement
    4) Federal/State Agencies

References

[Reference any law, regulation or standard that applies to this policy. **For Example**: 42 C.F.R. §§ 422.564 and 423.564]

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