POLICY INFORMATION

Policy Title: Safeguards for Sensitive Information, PHI and ePHI Policy and Procedure

Departmental Owner: Chief Compliance, Audit, and Privacy Officer

Version Effective Date: 2/28/24

Last Reviewed: 2/28/24

SCOPE

This policy applies to the following individuals and/or groups:

☒All of the below categories

☐All Employees ☐CT Employees ☐NY Employees ☐Remote Employees ☐Contractors☐Volunteers ☐Students/Interns ☐Vendors

This policy applies to all above listed Nuvance Health workforce members including but not limited to the following locations:

☐All of the below entities

☐Nuvance Health Systems

☐ Danbury Hospital (including New Milford Hospital Campus)	☒ Health Quest Systems, Inc. "(HQSI)"	☐ Western Connecticut Home Care, Inc ("WCHN")
☒Northern Dutchess Hospital	☒ Health Quest Home Care, Inc	☐ Western Connecticut Health Network Physician Hospital Organization ACO, Inc.
☐Norwalk Hospital	☒ Hudson Valley Cardiovascular Practice, P.C. (aka The Heart Center) ("HVCP")	☐Western Connecticut Home Care, Inc
☒ Putnam Hospital	☒ Other HQSI-affiliated Entities Not Listed	☐ Other WCHN-affiliated Entities Not Listed
☒Sharon Hospital		☒Nuvance Health Medical Practices (NHMP PC, NHMP CT, ENYMS & HVCP)
☒Vassar Brothers Medical Center		

POLICY STATEMENT/PURPOSE

The purpose of this policy is to establish appropriate administrative, technical, and physical safeguards of Sensitive Protected Health Information including Protected Health Information ("PHI") and Electronic Protected Health Information ("ePHI") created, used, or disclosed by the members of the Nuvance Health and its affiliates ("Nuvance") Work Force.

DEFINITIONS

See HIPAA Glossary

Covered Individual: This term refers to all Nuvance Health workforce members, business affiliates, and agents. Workforce members shall include any of the following individuals at Nuvance Health: Members of the Nuvance Health Board and the boards of any Nuvance Health related entity; President/Chief Executive Officer; administrators; managers, officers; employees, affiliates; medical staff members; appointees; volunteers; personnel; interns; students, trainees, and any individual whose conduct is under direct control of Nuvance Health whether or not they are paid by Nuvance Health. Business Affiliates shall include any non-workforce member, contractor, independent contractor, vendor, person, subcontractor or third-party, who or that, in acting on behalf of Nuvance Health: (i) delivers, furnishes, prescribes, directs, orders, authorizes, or otherwise provides Federal healthcare program items and services; (ii) performs billing or coding functions; (iii) contributes to Nuvance Health's entitlement to payment under Federal

healthcare programs; and (iv) is affected by one or more of Nuvance Health's risk areas through the Business Affiliate's interaction with, or performance of their role, functions, and responsibilities or provision of contracted services at Nuvance Health. Agents include individuals or entities that have entered into an agency relationship with Nuvance Health. Agents fall under the category of either Workforce Member or Business Affiliate depending on their role, functions, and responsibilities.

POLICY

1. It is the policy of Nuvance to comply with the applicable provisions of the HIPAA Privacy Rule section 45 C.F.R 164.530 (c) (1). It is also the policy of Nuvance to apply appropriate administrative, technical, and physical safeguards to protect PHI from misuse, loss, tampering, or use by unauthorized persons.
2. This policy addresses safeguarding of PHI received, created, used, maintained, and/or transmitted regardless of form, format or medium in accordance with the minimum necessary requirements for any disclosures set forth by federal, state and local laws and pertinent internal policies related to release of information, identity verification and system access policies.
3. All Nuvance Covered Individuals are responsible for adhering to this policy by using only the minimum information necessary to perform his or her responsibilities, regardless of the extent of access provided or available, and identifying and limiting practices which are likely to result in incidental uses or disclosure of Sensitive Information, PHI or ePHI.

PROCEDURE

Sensitive and/or urgent PHI or ePHI intended strictly for use within Nuvance and is disclosed only to third parties as required by law. Unauthorized disclosure could seriously and adversely impact Nuvance or its patients, members, employees, partners and business associates. Examples of disclosures that require valid authorization or a legally justified purpose for the disclosure include:

- Sexually Transmitted Diseases ("STD") and HIV test results and/or treatment
- First means of notification for confusing or abnormal diagnostic results
- Behavioral health conditions
- Drug and alcohol abuse and/or treatment
- Child or adult abuse and/or neglect
- Domestic abuse
- Peer review or risk management information (consult legal counsel or risk management before disclosing this information)
- For marketing and fundraising purposes except when allowed by law and in accordance with Nuvance policies

1. THE FOLLOWING GUIDELINES ARE TO BE FOLLOWED BY ALL NUVANCE COVERED INDIVIDUALS WHEN CREATING, USING OR DISCLOSING SENSITIVE INFORMATION, EPHI OR PHI

A. All clinical and administrative departments Managers which create, use, disclose or receive PHI or ePHI which is Sensitive Information are required to identify practices within their departments which are likely to result in and/or have resulted in incidental uses or disclosures of Sensitive Information, PHI or ePHI.
B. Once the practices are identified, each department manager is responsible for identifying safeguards which are reasonable in light of the nature of the Sensitive Information, PHI or ePHI, the department's operational needs, and the department's physical configuration. Administrative and financial considerations may also be taken into account in assessing the reasonableness of a safeguarding strategy.

C. Physical safeguards for Sensitive Information, PHI or ePHI in verbal form might include (but are not limited to):
   1) Using discretion when conducting phone conversations with patients while others are within earshot.
   2) Conducting routine discussions among clinicians (e.g., change of shift, rounds, etc.) in a private area where patients or unauthorized individuals cannot overhear.
   3) Using a low voice when communicating with patients in places where the conversation might be overheard or, alternatively, maintaining a space for private patient conferences.
   4) Seeking the patient's permission before discussing the patient's PHI in front of visitors.
   5) Refraining from discussions whose context would allow a listener to identify the patient in question.
   6) When collecting or updating information during admission, using a form for patients to complete, rather than asking the questions aloud.
   7) Limiting the amount of information disclosed on a voice mail / answering machine or provided to individuals who answer the phone in the patient's absence at the telephone number provided by the patient to:
      - name,
      - telephone number,
      - entity name, and
      - brief message to have the patient call you back.

   When practical, determine in advance if it is acceptable to the patient to leave messages on answering machines or with other individuals in the household upon their absence. Note such acceptance in the patient's medical record.

D. Physical safeguards for Sensitive Information, PHI or ePHI in written or electronic form might include (but are not limited to):
   1) Shredding or destroying any patient care forms, labels, addressograph chips, bracelets, and other documents or discarding them only after redacting (or crossing out) any Sensitive Information or PHI;
   2) Using "privacy screens" to conceal Sensitive Information, PHI or ePHI on computer screens; alternatively, placing and orienting computers in such a way as to conceal them from the view of passers-by;
   3) Keeping counters, desks, nurses' stations, and other surfaces clear of patient charts and other working documents;
   4) Configuring patient care areas to limit access to non-patients;
   5) Ensuring that fax machines and printers that may be used to transmit or receive Sensitive Information or PHI are not accessible to the public; and
   6) Abiding by reasonable restrictions on communications requested by patients, such as refraining from sending appointment reminders.

E. Proposed changes in operations, space configurations, or other circumstances should be assessed against this policy to ensure adequate and appropriate safeguards are utilized in accordance with this Policy.

2. THE FOLLOWING GUIDELINES ARE TO BE FOLLOWED BY NUVANCE COVERED INDIVIDUALS WHILE OUTSIDE OF THE WORKPLACE

A. Sensitive Information, including PHI and ePHI, is not to be removed or accessed by members of the Workforce without prior approval from their respective Vice President, or their designee and a signed confidentiality agreement.
B. The Workforce Member is responsible for maintaining the privacy and security of all Sensitive Information, ePHI or PHI that they may create use or disclose while transporting, storing or accessing off-site.
    1) Originals must not be taken off-site. Copies should be made for transport and should be shredded when no longer needed.
    2) All PHI taken off site must be locked in a suitable container such as a locking file box or briefcase.
    3) A log should be kept of all PHI taken off-site.
    4) Any Confidential Information or ePHI sent outside of Nuvance from workstations, laptops, PDAs and other mobile devices must be encrypted and password protected.
    5) Electronic media and printed information must be transported and stored in a secure manner.
    6) All media containing PHI or ePHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, faxes, hard drives, diskettes, flash drives, CDs, and DVDs.
    7) Nuvance materials must be secured when not being used and kept in a location that is not accessible to unauthorized persons.
C. Mobile Device Safeguards and HIPAA Security Protection
    1) Anti-virus software must be installed on all home computers and mobile devices used for Nuvance business, and they must be password protected and computer work data encrypted.
    2) Employees are required to maintain updates to current operating systems.
D. Confidentiality
    1) Passwords must not be shared or accessible to co-workers, family members or others.
E. The printing of Sensitive information, PHI, or ePHI from home computers should be kept to a minimum.

ENFORCEMENT

All individuals whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Failure to comply with this policy and related procedure may result in remedial and/or disciplinary action, up to and including termination of any employment or other relationship.

REFERENCES

45 CFR, Parts 160 and 164.530

Minimum Necessary for Use and Disclosure
45 CFR 164.528

APPROVAL

DocuSigned by:
Jared B Gaynor
6D04982F5DB24D1...

Signature

2/28/2024

Date

Original Effective Date: LHQ= 4/15/03
Revision Dates: 2/28/24
Supercedes: HQ 5.2.15 Safeguards for Sensitive Information, PHI and ePHI Policy;
HQ 5.2.15 Safeguards for Sensitive Information, PHI and ePHI Procedure