POLICY INFORMATION

Policy Title: Breach Notification 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: (i) outline Nuvance Health ("Nuvance")'s procedure when responding to potential or actual breach of protected health information, private information and other confidential personal patient or employee information; and (ii) to ensure that covered individuals understand their responsibilities related to: (a) the reporting of potential privacy and security incidents; and (b) Nuvance breach notification procedures.

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

Nuvance is committed to: (i) promptly investigating all instances involving the: (a) unauthorized access, acquisition, use or disclosure of protected health information ("PHI") and other confidential personal information; and (b) inadvertent loss of confidential personal information; (ii) mitigating risks that evolve from privacy incidents involving confidential personal information; and (iii) as required by internal policies and procedures or applicable Federal and State law, promptly reporting to affected persons, regulatory bodies, and the media any breach of confidential personal information.

PROCEDURE

I. OVERVIEW OF THE HIPAA BREACH NOTIFICATION RULE

1. The HIPAA Breach Notification Rule requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.

Definition of Breach

2. A breach is, generally, the acquisition, access, use, or disclosure of PHI in a manner that is not permitted under the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed to be a breach unless Nuvance Health or one of its business associates, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following for (4) factors ("HIPAA Risk Assessment"):
    - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    - The unauthorized person who used the PHI or to whom the disclosure was made;
    - Whether the PHI was actually acquired or viewed; and
    - The extent to which the risk to the PHI has been mitigated.

3. There are **three exceptions** to the definition of "breach."
    - The first exception applies to the unintentional acquisition, access, or use of PHI by a covered individual or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
    - The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.
    - The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

4. When conducting a HIPAA Risk Assessment to determine if a privacy incident constitutes a breach of PHI, the Nuvance Corporate Compliance Office ("Compliance") will: (i) contemplate and consider all of the exceptions, exclusions, factors, and elements set forth in the Breach Notification Rule and interpreting the United States Department of Health & Human Services ("HHS") guidance; and (ii) satisfy the following five (5) point criteria:
    - Conduct a risk analysis that is thorough and appeared to be conducted in good faith;
    - Perform a HIPAA Risk Assessment that at the minimum included the four (4) factors listed in § [I], ¶ 2 above;
    - Contemplate and consider, as necessary, factors beyond the four (4) regulatory factors listed above to appropriately assess the risk that the PHI has been compromised;
    - Conduct a HIPAA Risk Assessment that is consistent with an objective evaluation of the risk to the PHI in the matter at hand; and
    - Reach reasonable conclusions regarding the probability of whether PHI in the matter at hand was compromised, and such conclusions appeared to be derived from a diligently performed HIPAA Risk Assessment process.

Unsecured PHI and Guidance

5. Covered entities and business associates must provide the required notifications if the breach involved unsecured PHI. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the United States Health and Human Services Secretary ("Secretary") in guidance.

6. Encryption and destruction are the technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Breach Notification Requirements

7. Following a breach of unsecured PHI, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

A. Individual Notice

8. Covered entities must notify affected individuals following the discovery of a breach of unsecured PHI. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically and such agreement has not been withdrawn.

9. If the covered entity has insufficient or out-of-date contact information for ten (10) or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least ninety (90) days or by providing the notice in major print or broadcast media where the affected individuals likely reside. The covered entity must include a toll-free phone number that remains active for at least ninety (90) days where individuals can learn if their information was involved in the breach. If the covered entity has insufficient or out-of-date contact information for fewer than ten (10) individuals, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

10. Individual notifications must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and must include, to the extent possible, the following information:
    - a brief description of the breach;
    - a description of the types of information that were involved in the breach;
    - the steps affected individuals should take to protect themselves from potential harm;
    - a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches; and
    - contact information for the covered entity (or business associate, as applicable).

11. With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Such delegation is at the sole discretion of Nuvance, upon obtaining prior approval of the Chief Compliance Officer in consultation with the General Counsel. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual.

B. Media Notice

12. Covered entities that experience a breach affecting more than five-hundred (500) residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and must include the same information required for the individual notice.

C. Notice to the HHS Secretary

13. In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured PHI. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects five-hundred (500) or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than sixty (60) days following a breach. If, however, a breach affects fewer than fivehundred (500) individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than five-hundred (500) individuals are due to the Secretary no later than sixty (60) days after the end of the calendar year in which the breaches are discovered.

D. Notification by a Business Associate

14. If a breach of unsecured PHI occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than sixty (60) days from the discovery of the breach. To the extent possible, the

business associate should provide the covered entity with the identification of each individual affected by the breach as well as any other available information required to be provided by the covered entity in its notification to affected individuals.

Law Enforcement Delay

15. If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate must document in writing and specify the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or if the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

Administrative Requirements and Burden of Proof

16. Covered entities and business associates, as applicable, have the burden of demonstrating that all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach. Thus, with respect to an impermissible use or disclosure, a covered entity (or business associate) should maintain documentation that all required notifications were made, or, alternatively, documentation to demonstrate that notification was not required:
    - its HIPAA Risk Assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure; or
    - the application of any other exceptions to the definition of "breach."

17. Covered entities are also required to comply with certain administrative requirements with respect to breach notification. For example, covered entities must have in place written policies and procedures regarding breach notification, must train covered individuals on these policies and procedures, and must develop and apply appropriate sanctions against covered individuals who do not comply with these policies and procedures.

II. STATE BREACH NOTIFICATION REQUIREMENTS

In addition to federal breach notification requirements, Nuvance is committed to providing, in a timely fashion, all notices required under applicable State law including New York General Business Law § 899-aa and Connecticut General Statute § 36a-701b to: (i) persons affected by the breach; (ii) State regulatory oversight agencies; and (iii) as applicable, to major statewide media (i.e., newspapers, radio, and television).

III. ANTI-RETALIATION/WHISTLEBLOWER PROTECTION

Nuvance is steadfast in its protection of whistleblowers and strictly prohibits retribution, harassment, intimidation, or any other form of retaliation against any Nuvance covered individual, business affiliate, and agent, or other persons or entities that, in good faith, make a compliance report or complaint under this policy or otherwise participates in the Program, as further set forth in the *Nuvance Health Whistleblower Protection Policy*.

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

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414
New York State General Business Law § 899-aa
Connecticut General Statute § 36a-701b

APPROVAL

DocuSigned by:
Jared B Gaynor
6D04982F5DB24D1...

Signature

2/28/2024

Date

Original Effective Date: LHQ= 2/27/14
Revision Dates: 2/28/24
Supercedes: HQ 5.2.21 Breach Notification Policy and Procedure