Title: Breach Notification Policy
Date Created: March 1, 2015
Date Modified: July 3, 2025
Date Approved by CCN Board of Directors: June 10, 2025
Date Approved by CCC Board of Directors: September 23, 2025
Date Approved by IPA Board of Directors: September 23, 2025
Policy# PS1

Purpose:

To ensure reported Health Insurance Portability and Accountability Act of 1996 ("HIPAA") violations are evaluated to determine if a Breach notification must be filed with the Office of Health and Human Services or reported to a Covered Entity with which a Care Compass Network Entity is a Business Associate, as defined under HIPAA.

Definitions:

Affected Individual(s): All persons who are affected by Care Compass Entities' risk areas including Care Compass Entities' employees, officers, Directors, managers, contractors, agents, subcontractors, independent contractors, governing bodies, or third-parties, who or that, in acting on behalf of the Care Compass Entities: (i) delivers, furnishes, directs, orders, authorizes, or otherwise provides health or social care items and services under State, Federal, or Care Compass programs; and (ii) contributes to the Care Compass Entities' entitlement to payment under Federal health or social care programs, or from other payor sources.

Breach: The impermissible acquisition, access, use or disclosure of PHI which compromises the security or privacy of such information. A breach is not considered to have occurred if the information has been de-identified, in accordance with the HIPAA Privacy Rule. There are limited exceptions to the definition of "breach."

1. The unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the Care Compass Entities or Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority. The information cannot be further used or disclosed in a manner not permitted by HIPAA.
2. The inadvertent disclosure of PHI by a person authorized to access PHI held by the Care Compass Entities or a Business Associate to another person authorized to access PHI held by CCN or a Business Associate, or organized health care arrangement in which the Care Compass Entities participate. The information cannot be further used or disclosed in a manner not permitted by HIPAA.
3. The Care Compass Entities 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.

Business Associate: A person or entity that, on behalf of a Covered Entity, performs or assists in performance of a function or activity involving the use or disclosure of PHI.

Care Compass Entities: Organizations that are directly, or indirectly through one or more intermediaries, owned or controlled by, or are under common ownership or control of, Care Compass Network, including Care Compass Collaborative, Inc. and Care Compass Supporting IPA, LLC .

Covered Entity: Health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions covered by the HIPAA Privacy Rule.

Individually Identifiable Health Information: Information that is a subset of health or social care information, including demographic information collected from an individual, and:

1. Is created or received by a health or social care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical, social need, or mental health or condition of an individual; the provision of health or social care to an individual; or the past, present, or future payment for the provision of health or social care to an individual; and
    a. That identifies the individual; or
    b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI): Individually Identifiable Health Information, that is transmitted by or maintained in electronic media, or transmitted or maintained in any other form or medium (with exceptions, as described under 45 CFR §160.103), that relates to a person's physical or mental health, and his/her treatment or payment that can reasonably be used to identify an individual including, but not limited to:

1. Name;
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code;
3. All elements of dates (except year) for dates related to an individual, including birthdate, admission date, discharge date, date of death, and exact age if over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older);
4. Telephone numbers;
5. Facsimile numbers;
6. E-mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) addresses;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographs and any comparable images; and
18. Any other unique identifying number, characteristic or code.

Investigation: An evaluation that considers the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI, or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated (i.e., whether the information immediately was sequestered or destroyed).

Staff: Employees, contractors, agents, consultants, volunteers, and others who act on the Care Compass Entities' behalf.

Policy:

It is the policy of the Care Compass Entities to maintain privacy and security measures to protect the confidentiality of PHI by preventing impermissible acquisition, access, use or disclosure of such PHI. This Policy describes the process by which the Care Compass Entities identify, verify, notify, and address any such Breach of PHI.

I. Breach Notification – Care Compass Entities **Functioning as a Covered Entity.**

a. Pursuant to HIPAA, and the regulations promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (HITECH/Omnibus), as well as pursuant to applicable New York State privacy laws and regulations, including New York State General Business Law (§ 899-aa) and the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), the Care Compass Entities will notify individuals when an impermissible acquisition, access, use, or disclosure of PHI is determined to be a Breach, unless the risk assessment demonstrates a low probability that the PHI has been compromised.

b. Confirmed Breaches of the security or confidentiality of PHI will invoke certain actions by the Director of Compliance, who serves as Privacy Officer for the Care Compass Entities, and the applicable Compliance Committee(s) to determine the degree of risk and impact of the Breach upon an individual(s) and, under specific circumstances, notification of the Breach to the affected individual(s).

c. Affected Individuals shall report any potential Breach immediately to the Director of Compliance. The Director of Compliance will conduct an investigation into the potential Breach.

d. The investigation and steps will be thoroughly documented by the Director of Compliance. If the Director of Compliance concludes that no Breach has occurred, as that term is defined in HITECH/Omnibus, the Director of Compliance will recommend the appropriate corrective action based on the disclosure.

e. If the Director of Compliance confirms that a reportable Breach of security or confidentiality has occurred, the Director of Compliance will notify the Executive Director and the Chair of the applicable Compliance Committee on the date of discovery, conduct an analysis of the requirements for notification of the State in which the individual(s)

reside(s), and provide notification to individuals and required State and Federal agencies as indicated in this Policy and following the ENT_PS1-1 Breach Notification Procedure.

f. In an instance of a Breach, the Director of Compliance will, without unreasonable delay and in no case later than sixty (60) days following the discovery of a Breach:
    i. Notify affected individuals following the discovery of a Breach of unsecured PHI in written form;
    ii. Provide substitute individual notice by either posting the notice on the home page of the applicable Care Compass Entity website for at least ninety (90) days or providing the notice in major print or broadcast media where the affected individuals likely reside, if the Care Compass Entities have insufficient or out-of-date contact information for ten (10) or more individuals; or
    iii. Provide substitute notice by alternative form of written notice, telephone, or other means, if the Care Compass Entities have insufficient or out-of-date contact information for fewer than ten (10) individuals.
    iv. If the Breach occurs at or by a Business Associate of the Care Compass Entities, the Care Compass Entities may delegate the responsibility of providing individual notices to the Business Associate after considering which entity is in the best position to provide notices to the individual, which may depend on various circumstances, such as the functions the Business Associate performs on behalf of the Care Compass Entities and which entity has the relationship with the individual.

g. If any instance of a Breach involves less than 500 patients/clients, the Director of Compliance will:
    i. Notify the Secretary of Health and Human Services (HHS) of the Breach within sixty (60) days of the end of the calendar year in which the Breach was discovered;
        1. The Care Compass Entities are not required to wait until the end of the calendar year to report Breaches affecting fewer than 500 individuals and may, instead, report such Breaches at the time they are discovered.
    ii. Complete a separate notice for each Breach incident and submit the notice in the manner specified on the HHS website (https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html).

h. If any instance of a Breach involves 500 or more patients/clients, the Director of Compliance will:
    i. Without unreasonable delay and in no case later than sixty (60) calendar days after discovery of a Breach, notify the Secretary of HHS by submitting the Notice to the Secretary of HHS Breach of Unsecured Protected Health Information in the manner specified on the HHS website (https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html);
    ii. In an instance of a Breach affecting more than 500 residents of a State or jurisdiction, coordinate with the Marketing Manager, the Executive Director, and the applicable Compliance Committee for media notification, without unreasonable delay and in no case later than sixty (60) days following the discovery of a Breach, in the form of a press release to appropriate media outlets serving the affected area; and.

iii. Notify the Office of the New York State Attorney General (OAG), the New York Department of State, the New York State Police, and consumer reporting agencies of the timing, content and distribution of the notices, and approximate number of affected persons within five (5) business days of notifying HHS.
    1. Notification will be made automatically to required New York State offices and agencies, as well as applicable consumer reporting agencies, following submission of a breach form through the OAG's data breach reporting portal at https://formsnym.ag.ny.gov/OAGOnlineSubmissionForm/faces/OAGSBHome.

i. The Director of Compliance shall maintain documentation of the name of each individual notified, each log maintained by the Care Compass Entities, and any other notification to the Secretary of HHS, as required by law. Such documentation shall be retained for six (6) years.

j. The Director of Compliance shall report identified potential Breaches to the applicable Compliance Committee.

k. The Director of Compliance shall report confirmed Breaches to the applicable Compliance Committee and Board of Directors.

II. Breach Notification – Care Compass Entities Functioning as a Business Associate.

a. Affected Individuals shall report any potential Breach immediately to the Director of Compliance. The Director of Compliance will conduct an investigation into the potential Breach.

b. The investigation and steps will be thoroughly documented by the Director of Compliance. If the Director of Compliance concludes that no Breach has occurred, as that term is defined in HITECH/Omnibus, he/she will recommend the appropriate corrective action based on the disclosure.

c. If the Director of Compliance confirms that a reportable Breach of security or confidentiality has occurred, the Director of Compliance will notify the Executive Director and the Chair of the applicable Compliance Committee on the date of discovery and provide notification to the Covered Entity following the ENT_PS1-1 Breach Notification Procedure.

d. Pursuant to HIPAA, and the regulations promulgated thereunder, and the Health Information Technology for Economic and Clinical Health Act (HITECH/Omnibus), as well as pursuant to applicable New York State privacy laws and regulations, the Care Compass Entities will notify any applicable Covered Entity without unreasonable delay and in no case later than the number of days required within the Business Associate Agreement between the Care Compass Entities and said Covered Entity or 60 calendar days, whichever is sooner, after discovery of a Breach of unsecured PHI.
    i. Notification to the Covered Entity shall include, to the extent possible, the

identification of each individual whose PHI was, or reasonably believed by the Care Compass Entities to have been, accessed, acquired, used, or disclosed during the Breach.

ii. The Care Compass Entities shall provide the Covered Entity with any other available information that the Covered Entity is required to include in notification to the individual, or promptly thereafter as information becomes available.

e. The Director of Compliance shall maintain documentation of the name of each individual involved in the Breach, each log maintained by the Care Compass Entities, and any other notification to a Covered Entity, as required by law. Such documentation shall be retained for six (6) years.

f. The Director of Compliance shall report identified potential Breaches to the applicable Compliance Committee.

g. The Director of Compliance shall report confirmed Breaches to the applicable Compliance Committee and Board of Directors.

CCN Board Approval History: 3/11/2015, 12/8/2015, 11/8/2016, 12/21/2017, 2/12/2019, 12/10/2019, 11/10/2020, 11/9/2021, 6/14/2022, 11/8/2022, 8/8/2023, 8/13/2024, 6/10/2025

CCC Board Approval History: 9/12/2023. 9/24/2024, 7/22/2025, 9/23/2025

IPA Board Approval History: 9/12/2023. 9/24/2024, 7/22/2025, 9/23/2025

Compliance Committee Review History: 12/8/2015, 10/28/2016, 11/17/2017, 1/18/2019, 11/15/2019, 10/16/2020, 10/15/2021, 5/13/2022, 11/1/2022, 7/28/2023, 7/24/2024, 5/22/2025, 8/21/2025

Policy Revisions:

Date	Revision Log	Updated By
3/1/2015	Original creation	Ann Homer
11/19/2015	Updated to reflect Care Compass Network organization structure	Rebecca Kennis
10/28/2016	Updated to reflect the removal of NYS Compliance governing bodies	Andrea Rotella
11/17/2017	Updated with changes by the Compliance and Audit Committee	Andrea Rotella
1/18/2019	Updated definition of "staff" and other changes by the Compliance and Audit Committee	Andrea Rotella
11/15/2019	Updated with changes by the Compliance and Audit Committee	Andrea Rotella
10/16/2020	Removed references to NYS DUA and MCD	Andrea Rotella
2/24/2022	Update to reflect CCN as a Business Associate	Andrea Rotella
7/14/2023	Updated Director of Compliance title throughout	Cathy Petrak
8/6/2024	Updated to an Enterprise-wide policy; updated section I(f) to include covered entity reporting obligations to the New York Attorney General and other state offices/agencies	Cathy Petrak

5/8/2025	Updated “Affiliated Entities” to “Care Compass Entities” throughout and added “Affected Individuals” definition and updates throughout	Cathy Petrak
7/3/2025	Updated Breach notification requirements for instances in which the Care Compass Entities are functioning as a Covered Entity	Cathy Petrak

This Policy shall be reviewed periodically, but not less than once every 12 months, and updated consistent with the requirements established by the Board of Directors, Care Compass Network’s Leadership Team, Federal and State law(s) and regulations, and applicable accrediting and review organizations.