Title: Information Security Program Management Policy
Date Created: July 25, 2016
Date Modified: December 6, 2022
Date Approved by CCN Board of Directors: August 8, 2024
Date Approved by CCC/IPA Board of Directors: November 12, 2024
Policy# PS17

Purpose:

This policy serves to establish the information security program management requirements for Care Compass Network (CCN) and its Affiliated Entities.

This policy pertains to Staff, vendors, community health teams, participating organizations and any other person who has access to CCN's and its Affiliated Entities' information systems or to PHI, PII, or to Sensitive Information.

Definitions:

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

Applicable Privacy and Security Laws: HIPAA, as defined below, and all other applicable federal, state, and local laws and regulations that govern the creation, storage, receipt or transmission of individually identifiable medical records or information.

Architecture: A set of related physical and logical representations (i.e., views) of a system or a solution. The Architecture conveys information about system/solution elements, interconnections, relationships, and behavior at different levels of abstractions and with different scopes.

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to CCN and its Affiliated Entities that the incapacity or destruction of such systems and assets would have a debilitating impact on CCN and its Affiliated Entities.

Critical Security Documents: Documents that are central to the management of the CCN and its Affiliated Entities Information Security Program Plan (e.g., results from independent program reviews, Security Assessments, Tests, and Audits Reports, and Security Incident Reports and Findings).

Enterprise Architecture: A strategic information asset base that defines the mission, the information necessary to perform the mission, the technologies necessary for performing the mission, and the transitional process for implementing recent technologies in response to changing mission needs. Enterprise Architecture includes baseline Architecture, target Architecture, and sequencing plan.

Essential Documents: Documents that are important to the management and health of the organization, such as contracts, personnel records, financial information, Critical Security Documents, and client/customer information.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as amended by the Health Insurance Technology for Economic Clinical Health Act (HITECH) and any regulations, rules, and guidance issued pursuant to HIPAA and the HITECH Act (collectively "HIPAA").

Identity and Assurance Level (IAL): The level of security controls required for establishing confidence in user identities electronically presented to an information system. This level is also utilized in establishing the level of security settings and controls required in each information System's Security Plan.

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

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- 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
- That identifies the individual; or
- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Protection Needs: Technology-independent, required capabilities to counter Threats to organizations or individuals through the compromise of information (i.e., loss of confidentiality, integrity, or availability).

Information Security Architecture: An embedded, integral part of the Enterprise Architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel, and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Information Security Program Plan: Formal documentation that provides an overview of the security requirements for CCN's and its Affiliated Entities organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements, in support of mitigating or reducing security and data protection risks identified in CCN's and its Affiliated Entities' mission/business plan.

Personal Identifiable Information (PII): Information that can be assumed to identify the individual person including, but not limited to:

- Names of patient, relatives, and employer.
- Address or address codes, email address, IP address, and Universal Resource Locator (URL).
- Birth date, telephone, and fax numbers.
- Social Security, Health Plan Beneficiary, Certificate, License, and Vehicle numbers.
- Medical Record or account numbers.
- Finger or Voice prints and Photographic or Diagnostic images.

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 including, but not limited to:

- Name.
- 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.
- 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).
- Telephone numbers.
- Facsimile numbers.
- E-mail addresses.
- Social Security numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) addresses.
- Biometric identifiers, including finger and voice prints.
- Full face photographs and any comparable images; and
- Any other unique identifying number, characteristic or code.

System Security Plans: Documentation that describes how CCN and its Affiliated Entities meet the security requirements for a system or how CCN and its Affiliated Entities plan to meet the requirements.

Sensitive Information: Information that relates to the organization's proprietary information or participating organizations' competitive information, including, but not limited to:

- Financial payments to participating organizations.
- Contract details with vendors, payors, or participating organizations.

- Any participating organization's proprietary information that could result in anti-competitive discussions or behaviors (including, but not limited to salary data, prices or pricing structure, strategic plans).
- Organizational compliance complaints and/or investigations; and
- Confidential employee information.

Staff: Employees, contractors, agents, consultants, volunteers, and others who act on CCN's and its Affiliated Entities' behalf.

Threat: Any circumstance or event with the potential adversely to impact organizational operations (including mission function, image, or reputation), organizational assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Policy:

I. Oversight. The CCN IT Director and CCN Information Security Officer is responsible for ensuring that security measures are assessed, developed, implemented, and maintained through an Information Security Program Plan to protect the confidentiality, integrity, and availability of PHI, PII, and Sensitive Information, under the guidance and oversight of the Information Technology, Informatics, and Data Governance Committee.

II. Information Security Program Plan.

a. An organization-wide Information Security Program Plan shall be developed and disseminated to appropriate individuals that:
   i. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
   ii. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
   iii. Reflects coordination among organizational entities responsible for the various aspects of information security (i.e., technical, physical, personnel, cyber-physical).
   iv. Comply with all applicable Privacy and IT Security Laws, other applicable IT security standards and frameworks, including HITRUST Control Objects, and CCN's and its Affiliated Entities' policies and procedures.
   v. Exclusions these standards and frameworks are documented, including reasons for exclusions, and managed Defines and addresses the Information Protection Needs arising from the defined mission/business processes.
   vi. Defines and addresses information security issues of critical infrastructure and key resources. Protection strategies are based on the prioritization of critical assets and resources; and
   vii. It is approved by the CCN IT Director and CCN Information Security Officer.

b. The Information Security Program Plan shall be reviewed and approved by the CCN IT Director and CCN Information Security Officer at least annually, or when there are significant changes in the environment.
c. An independent third-party assessor shall review the Information Security Program Plan at least annually, or when there are significant changes in the environment.
d. The Information Security Program Plan shall be updated to address organizational changes and problems identified during plan implementation or security control assessments.
e. The Information Security Program Plan shall be protected from unauthorized disclosure and modification.
f. The Information Security Program Plan may be represented in a single document or a compilation of documents at the discretion of the CCN IT Director and CCN Information Security Officer.
g. The CCN IT Director and CCN Information Security Officer or designee shall regularly report in writing containing information about the status of the Information Security Program Plan to the IT, Informatics, and Data Governance Committee, minimally including:
    i. Confidentiality of nonpublic information and the integrity and security of CCN's and its Affiliated Entities information systems.
    ii. CCN's and its Affiliated Entities cybersecurity policies and procedures.
    iii. Material cybersecurity risks to the organization.
    iv. Overall effectiveness of CCN's and its Affiliated Entities' cybersecurity program; and
    v. Material cybersecurity events involving the organization.

III. Security Policies and Procedures.

a. Security policies and procedures shall be developed and maintained, and supported by a controls framework that considers legislative, regulatory, contractual requirements and other policy-related requirements, consistent with AD1 – Policy and Procedures Administration Policy to support the Information Security Program Plan.
b. The security policies and procedures are regularly reviewed and updated, but no less than annually, to ensure they reflect leading practices (e.g., for systems and services development and acquisition), and are communicated throughout the organization to Staff in a form that is relevant, accessible, and understandable to the intended reader.
c. CCN and its Affiliated Entities shall ensure that individuals may make complaints concerning the information security policies, procedures, or the organization's compliance with its policies and procedures.
    i. The complaints and requests for changes shall be documented, and their disposition recorded, if applicable.
d. The CCN IT Director and CCN Information Security Officer shall be responsible for developing, reviewing, update (based on specific input), and approving security policies and procedures.
    i. Security policies shall be presented to the IT, Informatics, and Data Governance Committee for input, support, and recommendation to the CCN Board of Directors for approval.
e. The security policy and procedure reviews shall consider all appropriate elements that could impact the organization's risk profile, such as:

i. The changing nature of CCN's and its Affiliated Entities' operations and thus risk profile and risk-management needs.
ii. The changes made to the IT infrastructure of the organization, along with the changes these bring to CCN's and its Affiliated Entities' risk profiles.
iii. The changes identified in the external environment that similarly impact CCN's and its Affiliated Entities' risk profiles.
iv. The latest controls, compliance and assurance requirements and arrangements of national bodies and of new legislation or regulations.
v. The latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information.
vi. The results of legal cases evaluated in courts that thereby establish or cancel precedents and established practices; and
vii. The challenges and issues regarding the policies and procedures, as expressed to the CCN IT Director and/or CCN Information Security Officer by Staff and other key stakeholders.

IV. System Security Plans.

a. A System Security plan shall be developed for information systems that:
   i. It is consistent with CCN's and its Affiliated Entities Information Security Program Plan.
   ii. It is consistent with the CCN's and its Affiliated Entities Enterprise Architecture and the Information Security Architecture.
   iii. Explicitly defines the authorization boundary for the system.
   iv. Describes the operational context of the information system in terms of missions and business processes.
   v. Provides the security categorization of the information system including supporting rationale.
   vi. Describes the operational environment for the information system and relationships with or connections to other information systems.
   vii. Provides an overview of the security requirements for the system.
   viii. Identify any relevant overlays, if applicable.
   ix. Describes the security controls in place or plans for meeting those requirements, including a rationale for the tailoring and supplementation decisions; and
   x. It is reviewed and approved by the CCN IT Director and CCN Information Security Officer.
b. Copies of the System Security Plans shall be retained by the CCN IT Director and CCN Information Security Officer, and the system administrator(s).
c. System Security Plans shall be reviewed at least annually.
d. System Security Plans shall be updated, minimally every three (3) years, to address current conditions or whenever:
   i. There are significant changes to the information system/environment of operation that affect security.
   ii. Problems are identified during plan implementation or security control assessments.
   iii. When the data sensitivity level increases.

iv. After a serious security violation, due to changes in the Threat environment; or
v. Before the previous security authorization expires.

e. System Security Plans shall be protected from unauthorized disclosure and modification.
f. Security-related activities affecting the information system shall be coordinated with affected stakeholders before conducting such activities, to reduce the impact on other organizational entities.
g. System Security Plans may be represented in a single document or a compilation of documents, at the discretion of the CCN IT Director and CCN Information Security Officer.

V. Mission/Business Plan Considerations.

a. CCN and its Affiliated Entities' mission/business plan shall be defined with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.
b. Enterprise Architecture shall be developed with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations.

VI. Information Security Architecture.

a. An Information Security Architecture shall be developed that:
    i. Describes the overall philosophy, requirements, and approach to be taken regarding protecting confidentiality, integrity, and availability of organizational information.
    ii. Describes how the Information Security Architecture is integrated into and supports Enterprise Architecture; and
    iii. Describes any information security assumption about, and dependency on, external services.
    iv. Outlines the management of control baselines for systems
b. The Information Security Architecture shall be reviewed and updated, as necessary, or whenever changes are made to the Enterprise Architecture.
c. Planned Information Security Architecture changes shall be reflected in System Security Plans and organizational procurements/acquisitions.

VII. Information Security Resources.

a. Information Security Workforce:
    i. A senior information security officer (Security Officer) shall be appointed with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
        1. The Security Officer shall demonstrate professional competencies in security matters via a recognized security industry certification, and appropriate vendor certifications or a minimum of five years of security-related experience.
    ii. Dedicated information security workforce resources shall be employed in support of the Security Officer's management of the organization-wide information security program.

iii. An information security workforce development and improvement program shall be established and regularly reviewed, as defined in PS7 – Privacy and Security Awareness and Training Policy.

b. Information services budget requests shall include the resources needed to implement the information security program. Exceptions to this requirement shall be documented.
c. A business case should be created to request the required resources.
d. Information security resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them shall be identified and implemented for software and other technology.
    i. The information resources shall be updated based on changes in the inventory, or when other new or useful resources are found.
    ii. The Security Officer shall research and comply with industry standard Vulnerability Management standards and policies

VIII. Information System Inventory. An inventory of CCN and its Affiliated Entities information systems and assets shall be developed and maintained, as defined in PS15 - Asset Management and Media Protection Policy.

IX. Information Security Measures of Performance. Information security measures of performance shall be developed, monitored, and, when applicable, reported to the Information Technology, Informatics, and Data Governance Committee.

X. Security Authorization Process.
a. The security state of organizational information systems and the environments in which those systems operate shall be managed (i.e., documented, tracked, and reported) through security authorization processes.
b. Individuals shall be designated to fulfill specific roles and responsibilities within the organizational risk management process.
c. The security authorization processes shall be fully integrated into an organization-wide risk management program.

XI. Testing and Monitoring.
a. A process for ensuring that organizational plans for conducting security testing and monitoring activities associated with organizational information systems shall be developed and maintained and executed in a timely manner, as defined in PS8 - Systems Audit, Monitoring, and Accountability Policy.
b. Testing and monitoring plans shall be reviewed for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

XII. Plans of Action and Milestones.
a. Plans of action and milestones for the security program and associated organizational information systems:
    i. Are developed and maintained by the CCN Information Security Officer, or designee.
    ii. Document the remedial information security actions adequately to respond to risk to organizational operations and assets, individuals, or other organizations.

b. Plans of action and milestones shall be reviewed for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

XIII. Security Awareness, Training, and Directives.

a. A process for ensuring that organizational plans for conducting Security Awareness and Training activities associated with Applicable Privacy and Security Laws and current applicable security Threats shall be developed, maintained, and executed in a timely manner, as defined in PS7 – Privacy and Security Awareness and Training Policy.

b. Threat Awareness:

i. The CCN IT Director and CCN Information Security Officer, or designee shall establish and institutionalize contact with selected groups and associations (e.g., special interest groups, forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations.) within the security community:

1. To facilitate ongoing security education and training for organizational personnel.
2. To maintain currency with recommended security practices, techniques, and technologies; and
3. To share current security-related information including Threats, Vulnerabilities, and Incidents.

ii. Newly discovered security threats and vulnerabilities are quickly identified and mapped into CCN's and its Affiliated Entities security policies, guidelines, and daily operational procedures.

c. Security Alerts, Advisories, and Directives:

i. The CCN Information Security Officer, or designee shall receive information system security alerts, advisories, and directives from the United States Computer Emergency Readiness Team (US-CERT) or similar external agency on an ongoing basis.

ii. The CCN Information Security Officer, or designee shall generate internal security alerts, advisories, and directives as deemed necessary.

iii. The CCN Information Security Officer, or designee shall disseminate security alerts, advisories, and directives to applicable Staff, system administrators, the Information Technology, Informatics, and Data Governance Committee, and users of CCN and its Affiliated Entities information systems.

iv. The CCN Information Security Officer, or designee, in conjunction with CCN Leadership and system administrators shall implement security directives.

XIV. Essential Documents Protection and Retention

a. Essential Documents shall be protected from loss, destruction, and falsification through the implementation of security controls such as access controls, encryption, backups, electronic signatures, and locked facilities or containers.

b. Essential Documents shall be managed according to legal, regulatory, and business requirements for data retention, including:

i. Roles-based access controls and minimum-necessary access shall be used to prevent unwarranted access to Essential Documents.

ii. Specific requirements for retention and destruction of Essential Documents shall be identified and managed.
iii. Secure destruction of data when no longer needed for legal, regulatory, or business reasons shall be performed; and
iv. A process for identifying and securely deleting stored data that exceeds defined retention requirements shall be developed.

c. Security policies and procedures, and other Critical Security Documents shall be retained for a minimum of six (6) years from the date of their creation or the date when it last was in effect, whichever is later.
   i. Security policies and procedures shall be reviewed periodically, but no less than annually, and updated as needed, in response to potential Threats or environmental or operational changes affecting CCN's and its Affiliated Entities Information Security Architecture or Information Security Program Plan.
   ii. Security policies and procedures shall be made available to those people responsible for enforcing to which the policies and procedures pertain.

CCN Board Approval History: 9/13/2016, 12/21/2017, 11/13/2018, 12/10/2019, 02/09/2021, 02/08/2022, 02/14/2023, 8/7/2024, 11/11/2025

CCC/IPA Board Approval History: 11/12/2024, 11/19/2025

Committee Policy Review History: 11/08/2017, 10/18/2018, 11/21/2019, 01/21/2021, 01/20/2022, 01/19/2023, 7/17/2024, 11/10/2025

Policy Revisions:

Date	Revision Log	Updated By
7/25/2016	Original creation	Rebecca Kennis
11/21/2016	Added Policy Review History	Andrea Rotella
10/12/2018	Changed reference from DEAA to DUA	Dustin Moore
10/12/2018	Changed "Oversite" section to signify the IT & Data Governance Committee is utilized for Advisory and Guidance	Dustin Moore
10/28/2019	Per assessor recommendation removed "all" throughout policy	Dustin Moore
12/30/2020	Removed DSRIP Language and References, Added Security Plans definition; reference to PS7 - Security Awareness and Training Policy, reference to Security plan requirement to be compliant with Security Laws and Standards	Dustin Moore
10/25/2021	Added definitions for: Architecture, Critical Infrastructure, Critical Security Documents, Enterprise Architecture, Essential Documents, Incident, Information Protection Needs, Information Security Architecture, Threat, Vulnerability; Edited definitions for: Information Security Program Plan, System Security Plans; Moved "Security Alerts, Advisories, and Directives" section from PS5; Added Security Policies and Procedures, Essential Documents and Protection sections; Moved Risk Management Strategy section to CC1, Added requirement details to Information Security Resources section.	Rebecca Kennis

12/6/2022	Updated Information Security Program Plan requirement statement to include the allowance of a designee to report to the IT Governance Committee.	Dustin Moore
6/17/2024	Added Affiliated Entities definition, Updated Staff definition; converted policy to enterprise-wide policy, Updated Job Title for Senior IT Manager, Added Security Program complies with Applicable industry standards and frameworks	Dustin Moore
9/30/2025	Added definitions for Individually Identifiable Health Information, and updated definition of PHI. Updated Job Title for IT Director. Updated management of control baselines and updated vulnerability management standards.	Dustin Moore Kim Loveless

This Policy shall be reviewed periodically, but no less than once every 12 months, and updated consistently 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.