Title: Information Technology Acceptable Use Policy
Date Created: June 27, 2016
Date Modified: September 30, 2025
Date Approved by CCN Board of Directors: November 11, 2025
Date Approved by CCC/IPA Board of Directors: November 19, 2025
Policy# IT1

Purpose:

This policy defines information technology (IT) requirements, actions, prohibitions, and acceptable use of Care Compass Network (CCN) and its Affiliated Entities' information technology devices, systems, and resources, which Staff must follow within technical controls and implemented security configurations. Inappropriate use exposes CCN and its Affiliated Entities to risks including virus attacks, compromise of network systems and services, and legal issues.

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").

Digital Media: A form of electronic media where data are stored in digital (as opposed to analog) form. Includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks.

Electronic Communication: Communications using electronic resources including, but not limited to, e-mail, telephones, voicemail, instant messaging, video conferencing systems, Internet, fax, computer workstations, mobile devices, and servers.

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:

- It 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.

Mobile Device: A computing and communication device that allows portability (can operate without the use of an external power supply) and has the capability to store and process information, such as notebook/laptop computers, personal digital assistants, smart phones, tablets, digital cameras, and other Wi-Fi-enabled devices, etc. Mobile devices do not include Portable Media (e.g., thumb/flash drives, external/removable hard disk drives, etc.)

Non-Digital Media: A form of media where data are stored in analog form. Includes, for example, paper and microfilm.

Participant: Any organization that has signed an Open Network Participation Agreement, an IPA Performance Network Participation Agreement, and/or an agreement related to a funded program with CCN and/or its Affiliated Entities.

Personally, 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.

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.

Smart Device: An interactive electronic device that understands simple commands sent by users and helps with daily activities. (e.g., smartphones, tablets, smartwatches, smart televisions, digital personal assistants, such as Alexa and Siri)

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

Unclassified Information: information that is not classified under specific laws or regulations but may still require safeguarding or dissemination controls. This type of information is often categorized as Controlled Unclassified Information (CUI), which is governed by laws and policies that dictate how it should be handled to protect sensitive data without classifying it as secret or top secret

Policy: This policy pertains to all staff, vendors, community health teams, participating organizations and any other persons who have access to CCN and its Affiliated Entities' information systems or to PHI, PII, or Sensitive Information.

I. Oversight. The CCN IT Director and CCN Information Security Officer is responsible for ensuring the protection of CCN and its Affiliated Entities' information systems environment by enforcing IT requirements, actions, prohibitions, and acceptable use of CCN, CCC, and/or IPA information technology devices, systems, and resources in support of industry standards, including HIPAA, HITECH and HITRUST requirements, under the guidance of the CCN IT, Informatics, and Data Governance Committee.

II. Prohibited Activities. Staff are prohibited from doing the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

a. Crashing an information system: Deliberately taking actions to make an information system or device unstable or inoperable prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred because of user action, a repetition of the action by that user may be viewed as a deliberate act.
b. Attempting to break into an information resource or to bypass a security feature: This includes, but not limited to, running password-cracking programs or sniffer programs,

removing, or disabling cyber security protection software, or attempting to circumvent file or other resource permissions.

c. Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
    i. Exception: Authorized information system support personnel, or others authorized by the CCN IT Director and CCN Information Security Officer or designer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
d. Browsing: The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a roles-based, "need to know" basis is prohibited.
e. Personal or Unauthorized Software: Use of personal software is prohibited. Software installed on CCN, and its Affiliated Entities' computers shall be approved by the IT Director and Information Security Officer or designed and installed only by authorized IT personnel.
f. Software Use: Violating or attempting to violate the terms of use or license agreement of any software product used by CCN and its Affiliated Entities is prohibited.
g. System Use: Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures, or business interests of CCN and its Affiliated Entities' is prohibited. CCN and its Affiliated Entities-owned systems and equipment shall not be used for nonwork-related functions without prior authorization from the CCN IT Director and CCN Information Security Officer.

III. Electronic Communication Resources Usage.

a. Electronic Communication resources and messages generated on or handled by CCN and its Affiliated Entities' -owned systems and equipment are considered the property of CCN and its Affiliated Entities' and not of individual users.
    i. CCN and its Affiliated Entities reserve the right, at its discretion, to review any Staff's files or messages created using Electronic Communications resources to the extent necessary to ensure electronic media and services are used in compliance with applicable laws and regulations, as well as CCN and its Affiliated Entities' policies.
    ii. Staff should structure Electronic Communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.
b. Communications must include an email signature at the end of the message containing the designated standard Staff information and confidentiality disclaimer.
c. CCN-provided Electronic Communication resources are intended for business purposes. Incidental personal use is permissible as long as:
    i. it does not consume more than a trivial amount of Staff time or resources.
    ii. it does not interfere with Staff productivity.
    iii. It does not preempt any business activity.
    iv. It does not consume more than a trivial amount of CCN and its Affiliated Entities' network resources.
    v. it does not violate any of the following:
        1. Copyright and reference law violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music,

books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.

2. Illegal activities – Use of CCN and its Affiliated Entities' information resources for or in support of illegal purposes as defined by federal, state, or local law is prohibited.
3. Commercial use – Use of CCN and its Affiliated Entities' information resources for personal or commercial profit is prohibited.
4. Political Activities –Political activities are prohibited on CCN, and its Affiliated Entities' premises and these activities must not be performed using CCN assets or resources.
5. Harassment –CCN and its Affiliated Entities prohibit the use of Electronic Communication resources in ways that are disruptive, offensive to others, or harmful to morale.
6. Junk E-mail - Communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited.
    a. If any of the above are received, the e-mail message shall be deleted immediately. The e-mail message shall not be forwarded.

IV. E-mail Security Controls

a. E-mails containing PHI, PII, or Sensitive Information sent over the Internet must be sent encrypted.
b. Prior to sending or receiving e-mails containing PHI, PII, or Sensitive Information, Staff must ensure that CCN and its Affiliated Entities have a signed Business Associate Agreement (BAA) or appropriate confidentiality agreement on file with the other organization.
    i. If Staff send or receive e-mails containing PHI, PII, or Sensitive Information that was not sent encrypted or was sent inappropriately, immediately report the incident to the CCN Privacy and/or Security Officer, or designees.
c. Outgoing e-mail messages to external e-mail addresses shall be scanned to check if the email contains PHI, PII, or Sensitive Information.
d. Unencrypted outgoing e-mail(s) that contain PII, PHI or Sensitive Information shall be blocked or shall alert the sender to use the secure email option.
e. The user and his/her supervisor shall be notified of any violations.
    i. The CCN IT Director and Information Security Officer and Compliance and Privacy Officer shall be notified of repeat offenders, who may receive disciplinary actions up to and including termination.

V. Internet Access.

a. Internet access provided by CCN and its Affiliated Entities should not be used for streaming entertainment videos, games, music, or other non-business, high-bandwidth activities.
b. Internet usage is monitored, and if a staff member is found to be spending an excessive amount of time or consuming substantial amounts of bandwidth for personal use, disciplinary action may be taken, up to and including termination.

c. Many Internet sites, such as games, unapproved file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by CCN and its Affiliated Entities' routers and firewalls. This list is constantly monitored and updated, as necessary.
d. Pornographic and gambling sites are prohibited from CCN and its Affiliated Entities' devices and Internet service. Any staff visiting pornographic or gambling sites will be disciplined, up to and including termination.

VI. Social Media Expectations and Requirements.

a. Staff are allowed to associate themselves with CCN and its Affiliated Entities' when posting on social media, but they must clearly brand their online posts as personal and purely their own. CCN and its Affiliated Entities shall not be held liable for any repercussions that such Staff content may generate.
b. Content pertaining to Sensitive Information, particularly when found within CCN and its Affiliated Entities' internal networks, should not be shared to the outside online community. Divulging information like the company's internal operations, legal matters, intellectual property, draft plans, or draft budgets, is strictly prohibited.
c. Content deemed dishonorable, as aimed at racial, ethnic, sexual, religious, and physical or disability groups, including slurs, slang, pictures, memes or re-posts, shares, or likes of such content will not be tolerated and may be considered a violation of organizational policy or anti-harassment requirements even when outside of normal work hours, and may result in disciplinary action.
d. In a personal post, content aimed at enriching understanding of racial, ethnic, sexual, religious, and physical or disability groups should be permitted, following organizational marketing protocols, to share how CCN and its Affiliated Entities have impacted these efforts.
    i. Staff should not share how CCN Participants have impacted these efforts, since this publication typically requires a press release.
    ii. Staff may like, share, or repost publications published from an official CCN or Participant social media account.
    iii. Staff should be skeptical of fraudulent news or any publication that portrays partial truths or publications from social media accounts from staff of an entity but not the entities direct social media account.
e. Social media posts, including direct publications, likes, shares, or re-posts of any kind, that slander, diminish, misrepresent, or sarcastically demean CCN and its Affiliated Entities' or its Participants' mission, vision, or goals are prohibited. Staff of CCN and its Affiliated Entities who have grievance should engage in the organizational grievance process.
f. CCN and its Affiliated Entities' reserve the right to require Staff to edit, amend or delete any post violating the CCN Code of Conduct or this policy. Failure to comply with this policy may result in progressive disciplinary action, including termination.
g. CCN and its Affiliated Entities shall authorize designated staff members to post information onto a publicly accessible information system on the organization's behalf:
    i. Prior to authorization staff are trained to ensure that publicly accessible information does not contain nonpublic information.

VII. CCN –Owned Mobile Devices

a. Mobile Devices shall be kept physically secured, when not in use.
b. Mobile Devices shall not be used by anyone other than the assigned user.

c. Only approved applications and software should be installed. Devices should not be "jailbroken" or rooted.
d. Devices must be protected by a strong password or PIN that meets company guidelines, and users must never share these credentials.
e. Mobile Devices are prohibited from connecting company devices to unsecured Wi-Fi networks

VIII. Personal Devices.

a. Staff may access the CCN WIFI guest wireless Internet service on their personal devices.
    i. Restricted activities referenced elsewhere in this policy also apply to activities performed on personal devices.
b. Staff are prohibited from connecting personal devices to the CCN and its Affiliated Entities' business network through Wi-Fi or a direct physical connection to the business network.
c. CCN and its Affiliated Entities reserve the right to restrict activities if they consume more than a trivial amount of Internet resources or are suspected to pose a threat to the CCN and its Affiliated Entities' business network.
d. Staff may request access to CCN and its Affiliated Entities' e-mail or select CCN and its Affiliated Entities' systems approved by the CCN IT Director and CCN Information Security Officer on their personal device(s), only after that staff member has signed and returned a Personal Device Agreement to the IT Department.
    i. Personal devices must employ available security mechanisms, including but not limited to password protection.
    ii. Personal devices with access to CCN and its Affiliated Entities' systems or data must be updated regularly with the most current available version of the operating system.
    iii. Lost or stolen personal devices containing CCN and its Affiliated Entities' business information are subject to remote wipe technology by CCN and its Affiliated Entities to protect potentially breaching confidential or protected information.
        1. Staff are required to notify CCN IT Department immediately if a personal device containing Sensitive Information is lost or stolen.
        2. An excessive number of incorrect logins from a personal device may trigger remote locking or remote wipe of that device.
    iv. Personal devices shall not store PHI or PII.
    v. Personal devices that access CCN and its Affiliated Entities' systems or data must be protected with an active security system, firewall, virus protection, and the most recent security patches and upgrades, where applicable.
e. Staff accessing CCN and its Affiliated Entities' systems from personal devices must adhere to CCN privacy and security policies and procedures to ensure data privacy and security.
f. The use of unauthorized personal devices to access organizational information systems is prohibited.
g. Staff using personal devices to access CCN and its Affiliated Entities' systems assume risks of loss or damage to the device. CCN and its Affiliated Entities may choose to assist the staff member with troubleshooting issues with the device related to the access of CCN and its Affiliated Entities' system but is not responsible for problem resolution.

h. The use of personal Digital Media is prohibited. Smart Devices are prohibited from being used to access or store CCN and its Affiliated Entities' systems or data, unless expressly approved by the CCN IT Director/ Information Security Officer.

IX. Protection of Data.

a. Users of CCN and its Affiliated Entities' information systems that contain PHI, PII, or Sensitive Information shall secure the information by locking the session (such that the information on the monitor is concealed) or logging out of the system when not in direct sight of the workstation.
b. Users of the CCN and its Affiliated Entities' information systems that contain PHI, PII, or Sensitive Information shall be logged out of the system when the time-period of expected inactivity exceeds the time limit designated in the Identity Level Assurance (IAL) Matrix for the specified systems.
c. Lost or stolen Mobile Devices are subject to remote wipe technology by CCN and its Affiliated Entities to protect potentially breaching confidential or protected information.
    i. Staff are required to notify CCN IT Department immediately if a Mobile Device is lost or stolen.
    ii. An excessive number of incorrect logins may trigger remote locking or remote wipe of that device.
d. Confidentiality Pledge
    i. Users of CCN and its Affiliated Entities' information resources shall sign the Confidentiality Pledge prior to being provided with access to the information resources.
    ii. The agreement shall include the following statement, or a paraphrase of it:
        1. I understand that any unauthorized use or disclosure of information residing on the CCN, and its Affiliated Entities' information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.
        2. The Confidentiality Pledge shall include contact information for the Security and Privacy Officers.
    iii. Temporary workers and third-party employees shall sign a Confidentiality Pledge document prior to accessing CCN and its Affiliated Entities' information resources.
    iv. Confidentiality Pledge Forms shall be reviewed and signed by Staff upon hire and annually thereafter.
e. PHI, PII, or Sensitive Information shall not be stored outside the designated and approved system or other appropriately secured system approved by the CCN IT Director and CCN Information Security Officer.
    i. A list of CCN and its Affiliated Entities' approved systems and storage locations, including cloud-based services, for usage and the storage of company data shall be made available to Staff.
    ii. PHI, PII, and Sensitive Information shall not be stored on local hard drives or Digital Media, unless expressly approved by the CCN IT Director and CCN Information Security Officer for a defined business need.
f. Copy, move, print, fax, and storage of PHI, PII, or Sensitive Information is prohibited without a defined and approved business need when accessed remotely.
g. Digital Media containing PHI, PII, or Sensitive Information shall be sanitized according to applicable NIST guidelines after use by the IT Department.

h. If PHI, PII, or Sensitive Information is printed, the "secure print" option on the printer must be used and the printed copy must be removed from the printer immediately to prevent unauthorized access.
i. If PHI, PII, or Sensitive Information is sent or received by fax, a cover sheet shall be used, and the faxed copy shall be removed from the fax machine immediately to prevent unauthorized access.
    i. Prior to sending a fax containing PHI, PII, or Sensitive Information, the fax number shall be validated, and the intended recipient shall be contacted prior to sending the fax to ensure that the recipient is able immediately remove the faxed copy from the fax machine to prevent unauthorized access.
j. If PHI, PII, or Sensitive Information is viewed on a monitor, the user is required to ensure that the information cannot be viewed by unintended individuals.
k. Nondigital media containing PHI, PII, or Sensitive Information shall be discarded in appropriate secure containers and/or shredded.
l. PHI, PII, and other Sensitive Information shall be kept in physically secure locations.
m. PHI, PII, or Sensitive Information shall be secured when office areas are not occupied by locking office doors, as is available, and locking information in desk drawers or file cabinets.
n. Unclassified Information shall be managed, as if it contains PHI, PII, or other sensitive information, utilizing the highest security control restrictions and protections, until the data is formally classified

X. Passwords.

a. Information system users are responsible for maintaining the confidentiality of their computer access and passwords. If a person suspects the confidentiality of their or another person's access code has been compromised, they shall:
    i. Notify the CCN Helpdesk; and
    ii. Change their password or request the password to be reset.
b. Leaving password codes in visible or non-secured locations is prohibited.
c. Use of another person's access code is prohibited.
d. The use of dictionary words and names for password/ pass codes is prohibited.

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
6/27/2016	Original Creation	Rebecca Kennis
11/21/2016	Updated Appendix A	Andrea Rotella
2/6/2018	Updated Appendix A	Andrea Rotella

10/12/2018	Changed reference from DEAA to DUA	Dustin Moore
1/29/2019	Included Definitions for: Staff, PII, PHI, MCD and IAL; Added Section II, b. iv: Section IV, b., and I; Removed inactivity time limit and referenced IAL Matrix; removed Appendix A reference and appendix	Rebecca Kennis Dustin Moore
10/31/2019	Per assessor recommendation removed, "all"	Dustin Moore
11/5/2019	Added section IV "Social Media Expectations and Requirements"	Dustin Moore
12/30/2020	Removed DSRIP Language and References; Added Email Security Controls from PS6 – Systems and Communications Policy, Security Staff Contact info, Personal devices restricted from CCN Business Network	Dustin Moore
9/29/2021	Added definitions for Digital Media, Electronic Communication, Mobile Device, Non-Digital Media, Smart Device; Added Oversight section; Removed extraneous text throughout, Added Mobile Devices section; Updated requirements for personal devices, Updated Protection of Data section to include print, fax, destruction requirements from PS10, Moved Passwords section from PS3.	Rebecca Kennis
12/1/2022	Added language prohibiting the use of CCN-owned systems and equipment without prior approval; Added language requiring the use of e-mail signatures to identify the organization the Staff is working on behalf of	Dustin Moore
6/19/2024	Added Affiliated Entities and Participant definition, Updated Staff definition; converted policy to enterprise-wide policy; Updated Job Title for Senior IT Project Manager	Dustin Moore
9/30/25	Added definitions for Individually Identifiable Health Information, and Unclassified Information, updated definition of PHI. Added section for social media posting on behalf of Care Compass. Updated Job Title for IT Director. Added requirements for Unclassified Information management.	Dustin Moore Kim Loveless

This Policy shall be reviewed periodically, but no less than 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.