



# CODE OF CONDUCT



HEALTHTEAM ADVANTAGE

## TABLE OF CONTENTS

Business Integrity .....	2
Company Assets.....	2
Confidential Business Information .....	3
Conflict of Interest .....	3
Conferences & Seminars.....	5
Copyright Materials.....	5
Corrective Action .....	5
Decision-Making Framework .....	6
Drug & Alcohol Use .....	6
Emails & Electronic Communications .....	7
Gifts & Entertainment.....	8
Government Official Dealings .....	9
Investigation Process .....	9
Non-Retaliation .....	10
Outside Activities.....	10
Protected Health Information & Breach Notification .....	10
Record Retention .....	11
Safe Workplace .....	11
Social Media.....	11
Weapons.....	12
Workplace Violence .....	12
Acknowledgment: Healthteam Advantage’s Code of Conduct .....	13

## BUSINESS INTEGRITY

Care N' Care Insurance Company of North Carolina, Inc. d/b/a HealthTeam Advantage (HTA or the Company) is committed to conducting business with integrity and in compliance with all applicable laws and regulations. Success depends on each of us making and keeping this commitment and helping ensure that all of our stakeholders obtain the best from each of us now and in the future. As an organization that primarily conducts business with the federal government, the Company is obligated to comply with State and Federal requirements.

Conducting ourselves and our business with integrity will strengthen our compliance program helping to make it a core competency and a competitive advantage.

Demonstrating integrity in the workplace means making the best possible decision. You must be aware of the situation, be careful to safeguard member and Company information, avoid potential conflicts, use Company property appropriately, ensure accurate and complete recordkeeping, and do everything you can to keep a healthy and safe workplace.

The Code of Conduct governs the conduct of all employees, members of the Board of Directors (when acting on behalf of the Company), first tier, downstream, and related entities (FDRs), contractors, and all agents of the Company. This policy may be supplemented by parent company policies and procedures as needed.

## COMPANY ASSETS

The Company assets are to be used solely for the benefit of the Company. Employees are responsible for assuring that Company assets are used only for valid Company purposes and are not used to access or view prohibited websites or content, including but not limited to gaming and/or pornography. The Company reserves the right to monitor Internet traffic and retrieve and read any data composed, sent, or received through its online connections and stored in the computer systems. Users should not have an expectation of privacy regarding their use of assets or Internet access, and users expressly consent to such monitoring by the Company.

Company assets include equipment, inventory, corporate data, concepts, business strategies and plans, financial data, and other information about Company business. These assets may not be used to provide personal gain for employees or others.

Employees may not transfer any Company assets to other persons or entities, except in the ordinary course of business. In addition, employees are prohibited from using Company

assets to visit impermissible websites, including gaming and pornography. Doing so could result in disciplinary actions up to and including immediate termination of employment.

Employees should never share login and password information with another employee. At times, Information Technology (IT) may need access to the user ID(s) or password(s) to troubleshoot technical issues. Abuse or misuse of assets or Internet access provided is a violation of Company policy and may result in disciplinary action, up to and including termination of employment.

## CONFIDENTIAL BUSINESS INFORMATION

You are responsible for safeguarding Company and member information. The Company has controls in place to help mitigate the risk of unauthorized use and access to information, including protected health information. Be mindful of the information you have and use care with it. Employees should always lock computers when away from their workstations and lock cabinets and drawers at the end of the workday.

No employee or affiliate should discuss Company business practices, clinical situations, physician practices, or employee performance in any situation in which they might be overheard or is not intended for public knowledge. You must protect this information.

The Company maintains a system of internal controls that it believes provide reasonable assurance that transactions are executed following management's authorization and Conflict of Interest, which includes written policies and procedures and examination by a professional staff of auditors. All employees are expected to adhere to these policies and to cooperate fully with internal and external auditors.

## CONFLICT OF INTEREST

Employees and members of the Board of Directors shall conduct their personal and professional relationships, including interactions with third-party vendors, in such a way as to assure themselves, the Company, and the community that decisions made are in the best interest of the Company without the slightest implication of wrongdoing. The exercise of judgment is required to determine if a potential conflict of interest situation exists.

A conflict of interest exists when an employee has a financial or other interest that may influence or have the appearance of influencing their judgment, decisions, or actions relating to HTA, the employee is in a position to profit directly or indirectly through the application of their authority or knowledge, or if a friend or relative of the employee benefits or the Company is adversely affected in any way by the action, or accepts gratuities.

A person has a financial interest if the person has, directly or indirectly, through business, investment, or family:

- An actual ownership or investment interest in any entity with which HTA has a transaction or agreement, or
- An actual compensation arrangement with any entity or individual with which HTA has a transaction or arrangement (either independent of or in connection with HTA's compensation plan) or
- A potential or actual ownership or investment interest in, or compensation arrangement with which HTA is negotiating a transaction or arrangement.

Gratuities may consist of things of value given freely and without consideration, gifts, remuneration (in cash or kind), entertainment unrelated to business purposes, or other favors from any entity or individual that does or wants to do business with HTA under circumstances from which it could be inferred that such action was intended to or would influence a member of the Board of Directors or employees.

Examples of conflicts include:

- Holding a financial interest in a company, by either you or a member of your immediate family, with whom the Company does business and influencing the direction of more business to the outside company.
- Directing Company business to an entity where a friend or relative works.

Members of the Board of Directors and employees will:

- Seek guidance from their supervisor or the Compliance and Integrity Department when any questions arise about conflict of interest;
- Provide full disclosure to the immediate supervisor, Human Resources, or Compliance Officer of any knowledge of actual/potential conflict of interest before consummation of the transaction or at the point of awareness;
- Avoid any transaction where a conflict of interest is apparent;
- Avoid taking advantage of their position with HTA to advance personal interests;
- Complete the annual conflict of interest disclosure statement.

The Compliance Officer with members of management will:

- Review the conflict or potential conflict of interest; and
- Take action to remove any direct or indirect influence on decision-making that violates this policy.

HTA requires that all employees disclose any potential conflicts of interest at the time of hire and annually thereafter. Before taking any action that might raise a conflict of interest, you should seek guidance from your supervisor or the Compliance Department.

## CONFERENCES & SEMINARS

The Company recognizes that employees may need to be provided the opportunity for professional development and to earn continuing education credits for a degree or certification. The Company does not permit any outside entity or individual doing business with or wanting to do business with the Company from paying for an employee's expenses to attend a conference or seminar.

Prohibited expenses include, but are not limited to conference fees, airfare, lodging, meals, etc. An exception may be made for written contractual agreements or when speaking at a conference or seminar.

## COPYRIGHT MATERIALS

The Company strictly adheres to all agreements regarding the use and distribution of copyrighted material. The email system may not be used to share software, but it may be used to send files and information to authorized users following all such restrictions. The Company may be licensed for the use of programs or material with restrictions not to copy or distribute under the penalty of law. It will be each person's responsibility to adhere to all copyright restrictions. No software may be downloaded or installed without the prior knowledge and approval of the Company.

In addition, the illegal downloading and copying of copyrighted software and/or other copyrighted materials is prohibited. As a means of controlling Internet usage, the Company has a computer system firewall that logs all Internet usage and content. To ensure a virus-free environment, only the IT Department is authorized to download/install files and software from the Internet onto Company-owned devices.

## CORRECTIVE ACTION

The Company's Corrective Action Policy applies to issues of compliance misconduct. A violation of the Code of Conduct, Company Policies and Procedures, the law, or regulations may result in corrective action, including but not limited to termination of employment.

If an employee's work falls below acceptable Company standards, or the Company rules, Policies, or Procedures are not followed, this may result in disciplinary action. This

disciplinary action may be in the form of disciplinary warning steps or termination. The Company may choose to take one or more of these steps as necessary and may skip one or more steps progressing to immediate termination when it feels that circumstances warrant.

The level of corrective action will depend on factors such as the nature and severity of the issue and may result in any of the following levels of corrective action:

- Verbal Warning/Reprimand;
- Written Warning;
- Final Written Warning; and
- Involuntary Termination.

Unethical or illegal behavior that could impact our government business may subject the Company to governmental corrective actions. Corrective actions may include civil money penalties, sanctions such as suspension of enrollment, or formal notices of non-compliance.

## DECISION-MAKING FRAMEWORK

We are often faced with decisions involving integrity. When we are, it is helpful to have a framework to guide us through the potential issue. Here are some questions to help guide you:

- What is the potential issue and is it illegal or against the Company's policies and procedures?
- Who might be affected by the actions and how might they be impacted? This includes you, our stakeholders, and the Company.
- How might the potential issue affect me, the stakeholders, and the Company?
- Are the potential issues aligned with your personal ethics?

## DRUG & ALCOHOL USE

The Company strives to maintain a safe, healthy, and efficient working environment. The unauthorized or unlawful use, possession, sharing, sale, purchase, manufacture, distribution, transportation, or diversion of controlled substances by employees of the Company leads to safety and health risks, not only for themselves, but for others, and is prohibited. Reporting to work or being on duty (including break times and scheduled on-call time) while under the influence of alcohol or illegal drugs is prohibited.

If you suspect someone is impaired, notify your supervisor, Human Resources, or the Compliance and Integrity Department. The Company has an Employee Assistance Program in place to help employees who may have a substance abuse problem.

## EMAILS & ELECTRONIC COMMUNICATIONS

Email is a computer software application supplied to Company users as an aid to productivity and communication for business purposes. Email is intended only to benefit the Company and, therefore, any email failures will not give rise to damage claims by either Company affiliates or third-party users; by using email, the affiliate or third-party user acknowledges no right to a claim exists.

All electronic communications, whether sent within the Company or to persons outside the Company, should be courteous and professional in all respects and should not contain any statements that may violate the Company's harassment policies or that would embarrass the Company, its affiliates, or its customers. Email storage is a limited resource and is not to be used as a permanent storage facility. Emails may be automatically purged from the e-mail system without notice to employees at intervals established by the Company.

Email communications that are confidential or contain PHI are required to be encrypted by the employee when they are sent to outside entities. The Company has a system readily available for all employees to encrypt emails on a case-by-case basis. Employees simply need to write "Secure" in the subject line of an email that contains confidential or PHI. Not encrypting emails that contain PHI is a violation of Company policy and could result in disciplinary action up to and including termination.

Email sent or received on the Company's network is neither private nor confidential. The Company reserves the following rights:

- To monitor all email transmissions as needed to determine if the email is being used for other than legitimate business reasons and to protect the Company against copyright infringement, loss of trade secrets, or other business policy violations.
- To record and disclose to others all electronic communications at any time, with or without notice. No employee or other user of the email system has a privacy right in anything created, received, or sent on or from the email system.

Under certain circumstances, it may be necessary for the Company to review email messages or logs. Such circumstances include, but are not limited to:

- Suspected violations of Company policies or illegal activity.
- Litigation involving the Company that results in a subpoena for the production of documents, including email messages.
- Urgency in retrieving vital messages when an employee is not available to give his or her approval.
- Termination of employment.
- Upon request by management.

As a result, all employees should exercise extreme caution before sending information through the email system, as email messages are not private and can be intercepted by other parties. Email users should be aware that email messages can be monitored and recorded at any time and deleted emails may be restored. Email users should exercise extreme caution before sending email messages to parties outside the Company network; unless they are encrypted, such messages can be intercepted and read during transmission.

The Company's electronic communication systems exist for the legitimate business of the Company. Use of the electronic communication systems is prohibited for purposes that are not for the legitimate business of the Company. Incidental use of electronic communication systems for personal, non-business purposes is permitted in limited circumstances. Information on the systems is not private.

## GIFTS & ENTERTAINMENT

Gifts and entertainment raise many questions. Employees shall not be permitted to accept gifts, money, or other gratuities from outside individuals or entities. It is acceptable to accept small infrequent tokens of appreciation if the value of the item is under \$100.

Employees should not solicit meals or entertainment from any individual or entity. In some cases, it may be acceptable to accept meals and entertainment offered by outside individuals or entities in business dealings. These must be:

- Reasonable and not excessive.
- Infrequent.
- Compliant with Company, federal, and state laws; and
- Approved by management.

There may be instances when giving gifts and entertainment is acceptable but must still comply with the law and Company policies.

Never give monetary or nonmonetary gifts, either directly or indirectly, that might appear to influence, obtain, or retain business. Monetary gifts may include cash or cash equivalents (e.g., gift cards).

There are specific rules about gift-giving in government-related business. As a general rule:

- No cash or cash equivalent; and
- Medicare Advantage or Part D is limited to \$15 per item and \$50 per calendar year per individual.

For non-government businesses, employees may give nominal monetary and non-monetary gifts which should be primarily advertising in nature. General guidelines provide the gifts are limited to \$100 per year, per individual.

## GOVERNMENT OFFICIAL DEALINGS

Federal and State laws and regulations govern the Company's contacts with elected officials or their families. There are prohibitions on what can be offered by way of gifts, meals, entertainment, etc.

When interacting with government officials, cooperate fully and honestly with them in audits and inquiries. Always be truthful and accurate. Oral and documented representations made to the government must always be clear, accurate, complete, and not misleading. Employees should consult with the Compliance and Integrity Department on issues that involve these officials.

## INVESTIGATION PROCESS

All reports of potential or actual unethical behavior or non-compliance are immediately reviewed, and subsequent investigative action is taken as appropriate. During the investigation, the Compliance Department may seek assistance from other areas (e.g., Human Resources, Audit, Legal) to help ensure the investigation is conducted thoroughly and that any corrective and/or disciplinary action taken is consistent with the Company's Policies and Procedures.

Each of us is expected to cooperate fully with any investigation and keep it confidential. The compliance office supports an "open door" policy where anyone can bring forth a good-faith issue that will be treated in confidence.

## NON-RETALIATION

In many instances, the Company relies on you to report in good faith potential issues regarding compliance. The Company will not tolerate any retaliation, intimidation, discrimination, or other adverse actions when you are reporting potential issues. If you suspect or observe retribution or retaliation, report it immediately to your supervisor or via any of the methods.

Remember, knowingly and intentionally making false reports will also not be tolerated and will be subject to corrective action.

## OUTSIDE ACTIVITIES

The Company values and supports your involvement in the community. Sometimes these activities, including other employment, may have the potential to interfere with your work performance in a way that negatively impacts the Company. If you think that your outside activities interfere or may interfere with Company activities, talk to your supervisor or the Compliance Department.

## PROTECTED HEALTH INFORMATION & BREACH NOTIFICATION

The Company strives to maintain the confidentiality and security of all protected health information (PHI). If an employee becomes aware of a non-permitted disclosure (i.e. breach) of PHI from a member, provider, or vendor, report it immediately to:

- David Short, Vice President of Information Technology at [dshort@htanc.com](mailto:dshort@htanc.com), 276-340-5193
- Joleen Katula, Interim Vice President, of Compliance at [jkatula@htanc.com](mailto:jkatula@htanc.com), 336-790-4378
- Report anonymously 24 hours a day/7 days a week at [EthicsPoint](#), 855-741-4518

Timely notifications to the member and others as needed will occur. The care of each member is a personal, confidential matter, and protected health information (PHI) must not be discussed or disclosed to any unauthorized individual or in any other unauthorized fashion. An example of an intentional violation is researching, viewing, and/or sharing PHI for personal use that is not related to performing work duties. Any employee discussing or revealing confidential information will be subject to appropriate corrective action, up to and including termination, and may also be subject personally to federal penalties or prosecution.

The Company will also take reasonable steps to limit incidental uses and disclosure of PHI made according to an otherwise permitted or required use or disclosure such as: discouraging staff from discussing PHI anywhere except in a closed office; training staff and managers on the importance of confidentiality when dealing with PHI; encouraging employees to follow up with their health insurance carrier if they have questions about their own claims data and activity.

## RECORD RETENTION

Legal and regulatory practice require the retention of certain records for various periods, particularly in the tax, personnel, health and safety, environmental, contract, corporate, and government program areas. When litigation or a government investigation or audit is pending or foreseeable, however, all relevant records must not be destroyed until the matter is closed, and this may include drafts and copies as well as employee's notes and papers. Destruction of records to avoid disclosure in a legal proceeding may constitute a criminal offense. For all pertinent Medicare Advantage and Part D records related to the contract during the contract term, these records must be kept for up to 10 years from the final date of the contract period.

## SAFE WORKPLACE

All employees are expected to conduct themselves in a manner that promotes a safe cooperative, and professional environment and prevents disruptive behavior. You are expected to treat others with respect. The Company will not tolerate any harassment, abuse, intimidation, or other retaliation.

One of the ways we can help keep our environment safe is to display our badges while at work and be aware of anyone who is not wearing one. Access to Company facilities and restricted areas requires employees to show or scan their badge. Badges should always be worn above the waist while on Company property. If you notice someone who does not have a badge, ask them if they need assistance, and if needed, escort them to the reception office and do not allow them into operational areas of the Company.

If at any time, you observe any activity that violates the law or Company policy, contact your supervisor or building security immediately.

## SOCIAL MEDIA

We are committed to protecting privacy and maintaining an appropriate work environment. The use of social media should be consistent with all policies and procedures. We trust and expect you will use good professional judgment and personal responsibility at all

times. This includes participation in social media, including activity during and off work time and/or off the premises. Make sure you know and follow the related policies regarding privacy and employee conduct; you don't post anything on social media in the name of the Company without prior approval from management, and the equipment and work time should not be used to engage in personal social media activities. The use of Company computer systems is not private.

## WEAPONS

Weapons, concealed or otherwise, are forbidden on Company property except for on-duty and off-duty, sworn law enforcement officers with federal, state, or local jurisdiction, Armed Company/Private Police, or an Armed Transport Service (i.e., Loomis, Wells Fargo).

If you encounter anyone who has a weapon in their possession, you should immediately notify the building security.

## WORKPLACE VIOLENCE

The Company prohibits any disruptive, abusive, offensive, or impaired behavior. Prohibited conduct includes, but is not limited to:

- Inappropriate verbal communication, including profane, intimidating, or disrespectful language;
- Demeaning or condescending behavior, including condescending intonation, verbal abuse, or name-calling;
- Failure to adhere to Company Policies;
- Inappropriate physical contact, verbal outbursts, and physical threats;
- Unlawful workplace discrimination and harassment;
- Sexual harassment;
- Retaliation;
- Drug and alcohol use; and
- Violence in the workplace.

**ACKNOWLEDGMENT: HEALTHTEAM ADVANTAGE'S CODE OF CONDUCT**

I hereby acknowledge that I have read, understand, and will comply with the provisions of the HealthTeam Advantage Code of Conduct. I will seek guidance from and raise concerns about possible violations of this Code of Conduct with, my supervisor, senior management, or through the Compliance Hotline (EthicsPoint).

I will attend all required training provided by HealthTeam Advantage throughout the year.

---

Signature

Date

---

Employee Name (printed)

Title