Code of Conduct and Business Ethics

Network Responsibility & Compliance Program

Community Health Network
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Introduction — PRIIDE Values and Integrity</td>
</tr>
<tr>
<td>6</td>
<td>Why this is important</td>
</tr>
<tr>
<td>7</td>
<td>Reporting known or suspected compliance concerns</td>
</tr>
<tr>
<td>9</td>
<td>Patient rights</td>
</tr>
<tr>
<td>11</td>
<td>Employment practices and workplace conduct</td>
</tr>
<tr>
<td>14</td>
<td>Compliance with laws and regulations</td>
</tr>
<tr>
<td>17</td>
<td>Political, lobbying and community activities</td>
</tr>
<tr>
<td>20</td>
<td>Marketing practices</td>
</tr>
<tr>
<td>21</td>
<td>Responding to government inquiries</td>
</tr>
<tr>
<td>18</td>
<td>Financial matters</td>
</tr>
</tbody>
</table>
The true foundation of Community Health Network (the “Network”) has always been its commitment to provide quality care to our patients and to exceed the needs and expectations of all of our customers. We strive to ensure an ethical and compassionate approach to health care delivery and management and we must consistently demonstrate that we act with absolute integrity and compassion in the way we interact with our patients, physicians, suppliers, payers and one another.

Part of achieving the highest level of integrity possible is the adherence to all laws, rules, and regulations; network policies; accreditation, licensure, and certification standards; and ethical standards. To assist us, the Network has created the Network Responsibility & Compliance Program (NRCP) and appointed a Chief Risk and Compliance Officer.

This Code of Conduct and Business Ethics is a major step toward proudly and publicly proclaiming our commitment to our NRCP and to the standards and values that we have jointly committed ourselves to maintaining. This Code of Conduct and Business Ethics describes important responsibilities for each of us and empowers everyone to meet and exceed the expectations placed on us by the communities we serve. Each of us has an obligation to ensure a workplace culture that reflects our core values as well as our commitment to strong ethical principles and compliance with all applicable laws, rules and regulations.

Thank you for taking the time to read, understand and abide by this Code of Conduct and Business Ethics

Sincerely,

Bryan Mills  President and CEO  Community Health Network
Over many decades, the Network has built a reputation as a good corporate citizen and we enjoy a high level of public trust and confidence. Public trust and confidence are fundamental to good business and are a prerequisite for our continued success and our ability to continue to serve our customers. These are valuable assets that we cannot take for granted and must be safeguarded and earned every day.

In order to maintain our reputation for good citizenry and the public’s trust and confidence, we must conduct ourselves with the highest standards of integrity and fair dealing in everything we do as we serve our customers. This Code of Conduct and Business Ethics provides an overview of our NRCP and emphasizes the shared common values, which guide our actions. We are committed not only to the ideals reflected in this Code of Conduct and Business Ethics but also to assuring that our actions consistently reflect our words. In this spirit, we want to build a team with shared values. We expect everyone in our Network to reflect the high standards we have set. However, nothing can substitute for our own internal sense of fairness, honesty, and integrity.

If you encounter a situation in your daily work, or are considering a course of action that “just doesn’t feel right,” you should discuss the situation with your immediate supervisor. However, if you are not comfortable reporting concerns to your supervisor, you may contact the compliance liaison for your entity, a member of leadership, or the Network’s Chief Risk and Compliance Officer at 317.621.7324. In addition, the Network recognizes that some may want an anonymous way to express concerns. In this situation, the Network provides AlertLine 800.638.5071, which is available 24 hours a day, 7 days a week.

You are a valuable member of our Network. We ask you to assist us, and all of our customers, in supporting the values and principles, which are critical to achieving our mission.

We know that we can count on your support!

Sincerely,

Jackie Smith  |  Chief Risk and Compliance Officer  |  Community Health Network
Introduction — PRIIDE Values and Integrity

Employees can ensure that Community Health Network is operating in an ethical and legal manner consistent with our PRIIDE values (Patients First, Relationships, Integrity, Innovation, Dedication, Excellence) by following this Code of Conduct and Business Ethics. Consistent with our most important value of “patients first”, access to care, clinical judgment and decision-making shall not be compromised, nor patient care jeopardized, by financial considerations. By acting with INTEGRITY, we build strong relationships, the respect of the communities we serve, and the trust of all of our customers.

I nteract with all Community Health Network customers — patients/families, physicians and other health care professionals, employers, employees, regulators, accreditors, subcontractors and vendors — honestly and fairly.

N ever use Community Health Network assets, information, or relationships for unauthorized personal gain.

T reat all confidential information that belongs to Community Health Network or to any of our customers with the highest possible protection and respect.

E nsure that potential or suspected violations of Federal and State laws, rules, regulations; ethical standards; accreditation and licensure standards; and Community Health Network policies and procedures are brought to leadership as soon as they are known and that there are no acts of retribution or retaliation against those who have reported any possible violations.

G enerate records of all transactions and services honestly, accurately and on a timely basis.

R efrain from conflicts of interest, both real and perceived, and declare those that exist.

I nitiate and maintain processes that result in consistent compliance with all Federal and State laws, rules and regulations; accreditation, certification and licensure standards; and Community Health Network policies and procedures that govern how we conduct our business.

T reat all of our customers fairly, ensuring equal opportunity and freedom from discrimination, harassment, intimidation or violence of any kind.

Y our recognition that even the appearance of misconduct or impropriety can damage Community Health Network’s reputation and our ability to serve our customers.

When each of us follows this Code of Conduct and Business Ethics every day and in everything we do, we reinforce our commitment to our PRIIDE values and contribute to fulfilling our mission, “To simply deliver exceptional healthcare with every life that we touch.”
Everyone who is associated with the Network must comply with the NRCP, the Network’s policies and this Code of Conduct and Business Ethics. This compliance is a condition of employment, medical staff membership, and contracting with the Network.

The NRCP and the standards set forth in the Code of Conduct and Business Ethics will be enforced at all levels, fairly and without prejudice. Those individuals who knowingly violate or attempt to interfere with any aspect of this program may be subject to employment or legal actions, including but not limited to:

- Verbal coaching;
- Written counseling;
- Formal Notice of Corrective Action;
- Final Notice of Corrective Action;
- Discharge;
- Repayment to the Network; and/or
- Civil/criminal charges

The Network’s failure to abide by all applicable laws, rules and regulations can result in public embarrassment, destruction of our image, and distrust by our customers. In addition, the Network may be subject to, but without limitation:

- Lawsuits;
- Repayment of monies paid to federal health care programs (e.g., Medicare and Medicaid) plus penalties;
- The imposition of civil and/or criminal fines and penalties; and/or
- Exclusion from future participation in the federal health care programs.
Confidentiality and Non-Retaliation

The Network recognizes and supports the right of every individual to address potential violations of Network policies and procedures; laws, rules and regulations; or ethical standards and request guidance without fear of punishment or harassment of any kind.

If you report a known or suspected violation “in good faith” and request your identity not be shared as part of the investigation, your identity will be kept confidential to the extent permitted by law and to the extent it does not prevent investigation of the situation. “Good faith” means that the report is made in accordance with standards of honesty and sincerity, but does not require that the suspected violation be an actual violation.

Retribution or retaliation against anyone who, in good faith, reports a possible violation is strictly prohibited. If you believe you are being subjected to corrective action or retaliation because you reported a suspected potential compliance violation, you should immediately report this retaliation through an appropriate channel, including the Chief Risk and Compliance Officer.

Any employee who deliberately makes a false accusation with the purpose of harming or retaliating against another employee will be subject to corrective action, up to and including discharge of employment.

Reporting known or suspected compliance concerns
How to report violations

The Network encourages direct communication with your immediate supervisors. Your supervisor is responsible for creating and maintaining an environment that encourages and supports honest and open communication.

If you are uncomfortable reporting concerns to your supervisor or if your supervisor could be involved in the potential compliance violation, you can contact other Network leadership or the Network’s General Counsel’s office at 317.355.5831.

The Network also recognizes that occasions may arise when one may want an anonymous way to express concerns. In these situations, the Network provides AlertLine, which is available 24 hours a day, 7 days a week. The AlertLine number is 800.638.5071. You have the option to give your name or to remain anonymous. Either way you should call back to check on the status of the Network’s action and communicate with the Chief Risk and Compliance Officer.

NOTE: AlertLine is not to be used for emergencies.

Investigations and Corrective Actions

The Network is committed to investigating all reported concerns promptly and confidentially to the extent reasonably possible. The Network’s goal for these activities is to eliminate or address any problems that may need to be corrected.

The Chief Risk and Compliance Officer will coordinate any findings from the investigations and review and recommend corrective actions or changes that need to be made. Every individual subject to the NRCP is expected to provide full support for and cooperate with any investigation, monitoring, auditing or other inquiry the Network initiates.

Where an internal investigation substantiates a compliance violation, appropriate corrective action shall be promptly initiated. Appropriate corrective action may include prompt repayment of any overpayment amounts, notification of the appropriate governmental agency, institution of disciplinary action and/or implementation of oversight systems to prevent similar violations from recurring in the future.
Each patient has rights, which are founded in our tradition and history, our moral and ethical standards, and federal and state laws, rules and regulations.

We provide access to care and make clinical judgments and decisions based solely upon what is in the best interests of the patient, without respect to the patient’s ability to pay.

**Health Record Documentation**

The patient’s health record is the documentation of services provided to our patients. The record must be complete, accurate and consistent with documentation requirements of governmental health benefit programs and accreditation, licensure and certification standards.

Accurate and thorough documentation of the patient’s health history and treatment is critical to:
- planning and providing appropriate care;
- communication and continuity of care;
- supporting the claim for payment; and

**Key patient rights include:**

- access to care by qualified caregivers
- respect of personal values, beliefs and civil rights
- informed participation in care
- privacy and confidentiality
- expression of opinions/complaints and receipt of resolution
- holistic care at the end of life

- protecting the Network and employees against any legal action taken.

**Identity Theft Prevention Program**

Identity theft in health care can have a serious effect when medical information for one person is used to treat another person. The Network has processes in place to deal with cases of identity theft and mixed patient records. Employees should
be alert to possible identify theft. “Red flags” for identity theft that are most likely to be found in our Network include:

- Identification documents provided by a patient that appear to be altered or forged;
- Personal information not consistent with other personal identifying information, like inconsistent or mismatched addresses or different or mismatched Social Security numbers (SSNs), etc.;
- Duplicate SSN (SSN provided is the same as SSN submitted by another patient); and
- Patient health record doesn’t match physical examination or medical history reported by the patient (like a patient’s record showing history of a broken leg but the patient’s x-ray shows no previous breaks).

Employees should be aware of these “red flags” and immediately contact their supervisor or other appropriate person to investigate, following the facility’s incident reporting policy.

**HIPAA Privacy Rule**

In enacting the Health Insurance Portability & Accountability Act of 1996, as amended from time to time (HIPAA), Congress mandated the establishment of standards for privacy of individually identifiable health information. We have a strong tradition of safeguarding an individual’s private health information. However, in today’s world of electronics, protecting that information becomes more difficult.

Under the HIPAA Privacy Rule, individuals have rights regarding their protected health information (PHI). These rights were meant to give patients additional control over how their PHI is being used or disclosed. The patient rights outlined under the HIPAA Privacy Rule are:

- Right to request a restriction on how PHI is used or disclosed
- Right to confidential communication
- Right to access PHI
- Right to request an amendment of PHI
- Right to an Accounting of Disclosures
- Right to obtain a Notice of Privacy Practices

The Network has adopted a number of specific compliance policies and procedures addressing the HIPAA Privacy Rule that affect our operations.
Diversity and Equal Employment Opportunity

Our employees provide our Network with a wide complement of talents, which greatly contribute to the richness of our services and our success. We are committed to providing an environment in which everyone is treated with dignity, fairness and respect. We comply with all laws, rules, and regulations related to non-discrimination in all of our personnel actions including hiring, promotions, staff reductions, transfers, evaluations, recruiting, advertising, compensation, and corrective actions.

Harassment/Workplace Threats and Violence

In accordance with the Network’s values, all employees will be treated with respect, dignity and courtesy. Our Network is committed to providing a workplace free of all forms of discrimination and conduct which can be considered harassing, threatening, hostile, intimidating, coercive, or disruptive.

• Harassment: Degrading or humiliating jokes, slurs, intimidation, or other harassing conduct is not acceptable in our workplace. Any form of sexual harassment is strictly prohibited. Sexual harassment occurs when unwelcome conduct of a sexual nature becomes a condition of an employee’s continued employment, affects other employment decisions regarding the employee, and/or creates an intimidating, hostile or offensive working environment.

• Workplace Threats/Violence: Workplace threats/violence is any conduct, action, or behavior
which is offensive; causes an individual to fear for personal safety/ safety of others or property; or harms another person or property. Workplace violence includes robbery and other commercial crimes, stalking, violence directed at the employer, terrorism or hate crimes. In addition, the Network prohibits the possession of firearms, other weapons, explosive devices or other dangerous materials on Network property.

**Solicitations**

Solicitation is approaching someone with a request or appeal. Often, the request is to buy something or donate money for some purpose. Common types of solicitation are private businesses selling goods or services or charitable organizations trying to raise money.

We want to provide a work climate where employees know they are free from:

- interruption of their work;
- being overwhelmed with requests for money;
- being uneasy and feeling pressure to “give” or “buy.”

Some types of solicitations are all right. Persons may conduct an activity on Network property if it:

- has a proper, charitable purpose which the Network would support;
- is not done on a face-to-face basis; and
- does not interfere with the work environment or productivity.

Examples:

- Network supported events such as United Way drive, charitable walks, Foundation activities, and hospital Auxiliary activities
- Sale of Girl Scout cookies or school band candy (i.e., use of sign-up sheet in break room)

Solicitation that involves an entire organization within the Network must be approved by a senior leader.

**Forbidden Solicitations and Examples**

The following solicitations are not allowed on Network property.

- Activities that are not legal, such as “pools” and unlicensed raffles;
- Political activities that raise money (e.g., employee running for political office trying to raise money in the hospital);
- Outside companies soliciting without Network approval; and
- Private businesses (e.g., Pampered Chef, Avon, homemade items, Amway, etc.).

**Network Assets**

Network Assets are the equipment, supplies, services and employees made available and supported by the Network. These include, but are not limited to:

- telephone
- e-mail
- photocopiers
- facilities
- equipment
- supplies
- intellectual property and information
- an employee’s time, for which the Network pays

AlertLine 800.638.5071
Personal use of these items, including conducting personal business while at work, is considered inappropriate use of Network assets and is prohibited. Using Network assets for personal reasons can result in theft, unethical behavior and fraud.

**Document Retention**

Health records and business documents are the property of the Network, which has a legal obligation to maintain the records. The laws pertaining to confidentiality and record retention must be followed in the maintenance, storage and disposal of documents.

**Sanctioned/Excluded Individuals and Entities**

The federal government and state agencies pay for some of the services that the Network provides to patients. Individuals and/or entities may be debarred or suspended from participating in federal or state program for various reasons, including inappropriate use of federal or state funds. The Network will not knowingly employ or contract with any individual or business which is debarred or suspended from participating in these programs.

We take proactive steps to check the government’s lists of excluded and debarred providers to ensure that no employees, medical staff members, vendors or independent contractors have been placed on these lists. These individuals have a duty to inform the Network of any change in their eligibility to participate in government programs.

**Drug Free Work Place**

As a drug-free and alcohol-free workplace, the Network is committed to providing a safe environment for our patients, employees and visitors and complying with the 1988 “Drug Free Workplace Act.” As a result, the Network requires that employees not report to work when they are impaired by drugs or alcohol and that employees be able to perform all of their job duties.

Our Drug Free Work Place policy also prohibits the unlawful or unauthorized manufacture, distribution, dispensation, possession, sale, or use of controlled substances on our premises, in our vehicles, or while engaged in Network business activities. Medications prescribed for another individual and medications that are not used in accordance with the prescription or product instructions shall be considered illegally used.

**Health and Safety**

Network employees are expected to obey all state, federal and local environmental and workplace safety laws, regulations and rules, including those promulgated by the Environmental Protection Agency and the Occupational Safety and Health Administration.
The Network is committed to full compliance with all federal, state, and local laws and regulations applicable to our business and operations and we will conduct business with honesty, fairness, and integrity. All employees, medical staff members, other healthcare practitioners, and contract service providers must be knowledgeable about and ensure compliance with the laws and regulations that are applicable to their professional duties.

**Billing, Coding and Cost Reports**

We submit appropriate and accurate claims to all patients and third party payers for medical services provided. This means that we must accurately document medical services provided, seek reimbursement only for those services which are medically necessary and actually performed, and not submit claims for services that are excessive or otherwise not legally reimbursable. We also must not submit false, fraudulent or misleading claims to any payer.

Specifically, we commit that we will:

- Maintain appropriate documentation that supports billing for our services.
- Only bill for services according to medical necessity guidelines.
- Document, correct and report identified billing errors to the appropriate payer and any overpayments will be promptly refunded.
- Properly train staff and provide them with billing updates in a timely manner.
- Operate oversight systems designed to verify that claims are submitted only for services actually provided and that services are billed as provided. These systems will emphasize the critical nature of complete and accurate documentation of services provided.
- Ensure that cost reports submitted on behalf of the Network are accurate, complete and comply with applicable laws and regulations.
- Accurately bill for services furnished in locations both on and off the main hospitals’ campuses.
- Identify and appropriately address on the cost report costs for services or items provided by “related parties” or “under arrangement” as defined in Medicare regulations.

**Relationships with Referral Sources**

The Network is subject to various federal and state laws and regulations regarding financial arrangements with physicians and other referral sources. The federal Anti-Kickback Statute regulates offers, payments, solicitations and receipt of anything of value in exchange for referrals. There are also state and federal laws governing patient referrals by physicians, such as the Stark Law. The
Stark Law, when applicable, prohibits physicians from referring patients, whose care is reimbursable by federal funds, to an entity providing certain services if the physician or a member of the physician’s immediate family has a financial relationship with the entity, unless all of the requirements for one of the Stark Law’s exceptions are met.

An example of a Stark Law exception is the personal service arrangements exception. This exception requires

• the arrangement be in writing;
• the arrangement covers all services provided;
• the aggregate services do not exceed those that are reasonable and necessary for the legitimate business purpose;
• the term of the arrangement is for at least one year;
• compensation is set in advance, does not exceed fair market value, and is not determined in a manner that takes into account the volume or value of referrals or other business generated between the parties; and
• the services to be performed under each arrangement do not involve the counseling or promotion of a business arrangement or other activity that violates federal or state law. An example of an arrangement that would likely fall under this exception is payments made to an independent physician for medical director services.

The penalties for violating the Stark Law and/or Anti-Kickback Statute include substantial fines and penalties, potential criminal conviction and/or exclusion from participation in federal and/or state funded healthcare programs.

We abide by these laws when entering into any financial arrangement with referral sources. We will neither offer nor accept anything of value in return for making a patient referral. We will make no payment nor provide any other type of consideration to anyone with the expectation the payment or consideration is dependent upon the admission, recommendation or referral of patients.

Submission of Claims

Federal and state False Claims Acts make it illegal to knowingly file a claim with a government health benefit plan (like Medicare or Medicaid) that is not consistent with billing requirements or contains false or misleading information. This is considered fraud and abuse. The False Claims Acts allow individuals to report suspected fraud or abuse. This type of lawsuit is referred to a Qui Tam lawsuit. Individuals who file such a lawsuit, generally referred to as whistleblowers, can receive a percentage of any settlement amount or damages plus reimbursement of legal fees and expenses. Both the state and federal False Claims Acts protect employees who report suspected fraud in good faith from retaliation by their employers.

The following examples would violate state and/or federal False Claims Acts. Claims for services that:

• were not rendered or were rendered but were not appropriately supported by documentation in the patient’s health records or were not medically necessary;
• were not covered by the governmental health benefit plan or did not meet governmental program billing guidelines; or
• identifies providers other than the providers who rendered the services (although some exceptions exist).
Intellectual Property

Intellectual property is any trademark, service mark, invention or technique, as well as copyrighted material, proprietary information and patent owned by the Network. Examples include our logos and materials developed by employees as part of their job, also known as work for hire. We may only use the property when necessary for our jobs and only in a form and manner directed by the Network.

Copyright

The copyright laws protect an individual or organization’s expression in whatever form it takes. Examples include: articles, videotapes, music performances, training materials, pictures, software programs, databases, cartoons, advertisements, tests, and manuals. This means if you can see it, hear it, or touch it — it may be protected.

With some very limited exceptions, we do not have a right to use anything that is copyrighted without the owner’s permission.

Copyright misconceptions

• “I found it on the Internet, so it’s OK.” Wrong. Just because a piece of work is available on the internet, does not mean the copyright laws can be ignored.

• “If we give credit to the author/publisher, then we’re OK.” Wrong. Permission from the owner to reproduce his/her material is required. Giving credit is polite, but it does not make it OK under the copyright laws.

• “I’m making a lot of copies, but they’re for internal distribution only, so it’s OK.” Wrong. The copyright laws do not distinguish between internal use and external use.

• “It doesn’t have a copyright symbol, so it’s not subject to the copyright laws.” Wrong. The copyright symbol (©) is not required. All printed, written or recorded material is copyrighted.

• “We’ve been copying and re-using this assessment/test in our department for years. I’m sure someone got permission a long time ago.” Maybe. Confirm that permission has been granted. Document and record permissions granted on the material you are using.

• “I’m not copying it; I’m just scanning and sending it via e-mail, so it’s OK.” Wrong. Scanning and e-mailing is the same as copying and distributing. Permission from the owner is required.
Political activity can include running for office, making campaign contributions, actively supporting a candidate for office, and voting.

Lobbying is a form of political activity. Lobbying occurs when an individual, a group of individuals, or an entity seeks to influence legislators’ voting policies and other decision making in a manner that benefits the individual, group or business that they represent.

Community activity typically refers to volunteering and other service to fellow members of a neighborhood, town, city or state. However, community activity can be a form of political activity if the purpose or effect of the activity falls within the definition of lobbying or political activity (such as organizing a rally to support increased funding for schools).

The Network supports and encourages everyone to take part in political affairs and to vote in elections. However, employees must do this:

• as private citizens, making it clear they are not representing the Network;
• on their own time, not on or in any property or facilities owned by the Network; and
• without using Network assets, such as time, money, goods, services, and/or equipment.

Organized displays of political party affiliations are prohibited within the Network.
All activities pertaining to money or tangible and intangible Network assets fall within the scope of financial matters. The Network has established accounting controls, which ensure transactions are reported in the proper account and cost center and during the month in which the financial obligation occurs. All transactions are to be executed in accordance with Network policies and procedures, authorized by leadership, and recorded in a proper manner.

**Conflict of Interest**

An employee’s right to privacy with respect to personal investments, financial interests, and activities is highly respected. However, sometimes they might create, or appear to create, a conflict of interest. A conflict of interest arises when:

- an employee’s interest, that of a family member or someone with whom an employee lives conflicts, or appears to conflict, with the interest of the Network; or
- an employee’s outside activities could, or appear to, impair job performance, impartiality, or ability to make objective decisions in the best interest of the Network.

Situations that could involve conflicts of interest should be avoided or considered with caution and guidance from the Network. Any possible conflicts of interest should be reported to Network leadership in accordance with the Network’s Conflict of Interest policy. The employee is responsible for disclosing the conflict or potential conflict.

**Private Inurement/Benefit**

Private inurement and private benefit are elements of federal income tax rules. They exist when a not-for-profit entity makes its assets available to a for-profit entity or individual for less than fair market value. While private inurement applies only to “insiders” (usually managers or officers with influence over the use of company assets), private benefit applies to any for-profit organization or individual. Violating these tax laws may result in 1) the not-for-profit entity losing its not-for-profit income tax status, 2) criminal charges, 3) civil lawsuits, or 4) additional taxes for the person who receives the benefit. Private inurement or private benefit occur when a not-for-profit organization provides items or services to a for-profit entity for free or significantly less than others would pay.

Examples include, but are not limited to:

- office space or equipment
- billing, nursing, or other staff
- training for independent physicians’ office staff
Business Courtesies (Gifts & Entertainment)

Business courtesies are the giving and receiving of any type of entertainment or gifts, whether tangible or intangible, between the Network and a current, former, or potential customer.

Examples include, but are not limited to:
- cash or equivalents, such as gift certificates;
- payment for travel, lodging or costs to events;
- meals and entertainment;
- sporting and other event tickets; and
- exchange of products.

There are many reasons the Network generally does not give or receive business courtesies. For example, business courtesies may:
- create conflicts of interest or the perception of conflicts of interest;
- give the wrong impression to our customers;
- be a violation of federal and state laws, rules and regulations; or
- be inconsistent with the Network’s ethical standards and principles.

Receiving & Giving Business Courtesies:
- Employees may accept or give gifts or promotional items with a value of less than $50 each, limited to $300 per year;
- Employees may accept or give perishable or consumable gifts not exceeding the above dollar values. If the gift is for a department or group, the value cannot exceed $50 per person;
- Reasonable and appropriate meals and entertainment in the local community for legitimate business purposes are acceptable
- Attendance at vendor sponsored workshops, seminars and training sessions is permitted with written approval of a senior leader;
- Employees may never accept and keep or give cash equivalents (such as gift certificates);
- Employees may never accept and keep or give gifts or promotional items with a value more than $50.00;
- Employees may not ask for gifts;

What can employees do to help?
- Never agree to buy anything without proper authorization. Refer the vendor to the purchasing department.
- Always follow purchasing policies and procedures.
- Do not reveal Network prices outside the Network without approval.
- Never make a promise to any vendor. Only the Purchasing Department may make such commitments.
- Never sign a contract or legal document unless properly authorized to do so.

- Employees may not accept a gift that would influence or appear to influence their role as an employee of the Network or to influence relationships, referrals or decisions.

Purchasing and Materials Management

The Network purchases and manages equipment, supplies, and services that we need to serve our patients and customers. We have checks and balances protecting us from activities that are dishonest, illegal or inconsistent with our contractual agreements.
Marketing is the effort undertaken by the Network to help promote our products and services. We market our products and services through the media, the Internet, and participation in special events and sponsorships. We present only truthful, fully informative, and non-deceptive information in our marketing efforts, without violating patient confidentiality.

**Antitrust**

Antitrust laws are federal and state laws that are meant to protect the consumer by maintaining competition. Antitrust violations occur when competitors agree not to act as competitors but plan to control the market for their own benefit, to the detriment of the people who do business with them. Even where no agreement is reached between competitors, if the Network has discussions of sensitive information with its competitors, the Network may be accused of engaging in behavior that violates antitrust laws. Some examples of prohibited conduct include, but are not limited to:

- Competitors agree to the price that each of them will charge for the same products or services;
- Competitors divide-up customers or territories so that the consumer has only one company that will sell him the product;
- Competitors agree to not use a certain vendor, payer or other party. This can be a way to force the vendor or payer to give them special treatment; and
- Competitors agree to the wages each pays for specific job categories.

**Obtaining Information About Competitors**

The Network obtains information about other organizations, including its competitors, only through legal and ethical means such as public documents, public presentations, journal and magazine articles and other published and spoken information. The Network does not obtain proprietary or confidential information about a competitor through illegal means, nor seek proprietary or confidential information when doing so would require anyone to violate a contractual agreement such as a confidentiality agreement with a prior employer. Additionally, competitors should not, directly or indirectly, share rates or pricing information related to third party payer contracts.
Various external organizations may contact individuals associated with the Network to initiate a compliance-related inquiry. Employees will comply with, cooperate with and provide truthful responses to lawful and reasonable requests or demands made as part of a government investigation. Although the Network prefers that employees not answer questions without Network representation, you are free to do so. Employees are under no legal obligation to answer any questions and have the right to refuse. However, employees should always:

- be polite and courteous;
- cooperate in a professional and supportive manner;
- be truthful;
- contact your supervisor, or in the absence of your supervisor, legal counsel or a compliance liaison;
- respond to requests only as instructed by the Chief Risk and Compliance Officer or legal counsel;
- ask for identification and a business card so the Network has a record of the official’s name, phone number and who the official represents; and
- after the encounter write down everything that happened.

If you are given a search warrant

Be polite and courteous; contact your supervisor, a compliance liaison, safety & security and legal counsel.

Ask for identification and a business card to have a record of their name, phone number and the organization they represent.

Ask the person to wait for security and legal counsel. However, the person does not have to wait. If the person won’t wait, ask what they are looking for, check the search warrant, and direct them to the information.

Keep a record of all actions.

If you are given a subpoena

Be polite and courteous; contact your supervisor; a compliance liaison; or legal counsel.

Ask for identification and a business card (attach the business card to the subpoena).

Accept the subpoena, sign for it if requested, and record the date and time you received it.
If you have concerns about possible violations of this Code of Conduct and Business Ethics; Network policies and procedures; laws, rules and regulations; or ethical standards, contact your supervisor, the Chief Risk and Compliance Officer, or AlertLine.