



Nonprofit corporations and independent licensees  
of the Blue Cross and Blue Shield Association

## **Code of Business Conduct**

### **High Ethical Standards: The Key to Our Success**

Our Code of Business Conduct is part of our way of life at Blue Cross Blue Shield of Michigan and Blue Care Network. Corporate ethics and corporate compliance are related concepts, but not identical. Ethics are part of the culture of an organization. They provide a framework for decision making by guiding workforce members to always consider and do the “right thing.” This framework focuses on guiding workforce members on how and why to follow the rules. Compliance is the requirement that workforce members abide by federal, state and local laws, contractual obligations, Blue Cross Blue Shield Association standards, and Company policies.

You must strive to maintain these high standards as you conduct the Company's business. Maintaining these high standards is the key to our success.

The standards are explained below and require workforce members and others acting on behalf of the Company, to act with honesty, integrity and impartiality when dealing with customers, providers, vendors, regulators, competitors, community, fellow workforce members, and board and council members. To earn and keep their trust, you must make every effort to avoid even the appearance of illegal or unethical conduct. You must also take positive action to prevent or correct any improper conduct. This includes identifying and reporting known or suspected violations of the law, the Code of Business Conduct, and suspected fraud, waste, or abuse.

Senior leadership and the boards of directors are committed to providing avenues through which ethical issues may be raised, reviewed and resolved openly and honestly. Help is available when you have questions about how to maintain ethical standards.

### **Nondiscrimination**

- Each workforce member, officer and director has a responsibility to treat applicants, subscribers, members, providers, workforce members and members of the public in a nondiscriminatory manner.
- The Company strictly prohibits any form of discrimination in our health programs and activities based upon race, color, national origin, sex, age or disability.

The term “discrimination” includes, but is not limited to treating an individual less favorably than others because they belong to one of the protected classifications identified above.

### **Conflicts of Interest**

One of the more common ethical dilemmas we confront involves potential conflicts of interest.

- A conflict of interest exists when a person's personal interests and his or her business responsibilities are at odds. You need to avoid personal interests that might conflict with your loyalty to the Company or compromise your judgment on the job. It is extremely important to avoid actions that could even appear to be influenced by personal interests.

## Confidentiality

- The Company is required by state and federal law, and is strongly committed, to safeguard the confidentiality of personal and protected health information. Such information includes a member's medical history, treatment records, age or marital status. You may have access to this information only if you need it to perform your job and you may use and disclose it only as permitted or required by law and by our corporate health information privacy policy and procedures. Any breach of this obligation to maintain the confidentiality of protected health information will be viewed very seriously and will result in discipline, up to and including termination of employment.
- You must vigorously safeguard the Company's confidential or proprietary information. Confidential or proprietary information includes any information that is not generally disclosed outside the Company and that may be useful or helpful to our competitors. Examples include financial data, customer lists, business strategies and information or data that we have agreed by contract to maintain confidentially. To protect this confidential information from improper disclosure, follow these guidelines:
  1. Share confidential information with others only on a need-to-know basis
  2. Do not transmit corporate information to personal emails or unauthorized external parties
  3. Do not use a workforce member-owned device to capture or disseminate images or audio of any corporate data
  4. Ensure that disclosure of any confidential information to outsiders is approved by leadership and protected by an appropriate confidentiality agreement
  5. Avoid incidental disclosures of confidential information in conversations with suppliers, customers and others
- Workforce members must also respect and protect the trade secrets, proprietary and confidential information of other entities acquired prior to working for the Company. This confidential or protected information cannot be used by workforce members without the written consent of the owner. Confidential or protected information includes, but is not limited to the following: customer lists, patented products, methods, or processes, copyrighted materials or the trade or service marks of others. Questions regarding ownership issues and the use of confidential or protected information should be directed to [ComplianceOffice@bcbsm.com](mailto:ComplianceOffice@bcbsm.com).

## Gifts and Entertainment

- You may not give or accept any gift from a customer, vendor, supplier, provider, consultant, agent or competitor that could be perceived to influence the recipient's sound business judgment or to gain an unfair or improper advantage.

## Accounting and Reporting

- You need to ensure the integrity of the Company by accurately and truthfully recording corporate information, accounting and operating data by strictly following established accounting and business procedures. You may not for any reason cause false or artificial entries to be made in Company records. Examples of improper conduct include causing records to appear as though a transaction occurred when it did not, causing records to appear as though a transaction occurred at a different time than it truly did, or failing to report suspected fraud, waste or abuse.
- No Company officer or director, or any other person acting under his or her direction should

take any action to fraudulently influence, coerce, manipulate or mislead any independent public or certified accountant engaged in the performance of an audit of the financial statements of the Company for the purpose of rendering such financial statements materially misleading.

### **Political Activities**

- The Company encourages you to be a good citizen and to participate in the political process. However, if you participate in political activities on your own initiative, including making personal political contributions to candidates or political parties, make it clear that you are acting as an individual and not acting on behalf of the Company. You may not use any Company property, facilities or time of any other workforce member for any political activity. Workforce members involved in political activities should do so outside of working hours.
- Corporate political activity is highly restricted. The Company is prohibited by law from using its funds to support candidates for federal, state or local office. The Company receives federal funds under government contracts and must carefully monitor activities in this area to ensure that government funds are never used for political activities. A narrow exception to this rule allows use of Company funds to form a political action committee that may then make political contributions using voluntary donations from eligible workforce members.

### **Fair Dealing**

- Each workforce member, officer and director has a responsibility to deal fairly with customers, suppliers, competitors and workforce members. We must not take unfair advantage of anyone through manipulation, concealment, abuse of privileged or confidential information, misrepresentation of facts or any other unfair business practices.

### **Antitrust Laws**

- We must conduct Company business in a manner that helps maintain a free and competitive market. Activities that would restrain a competitive market, even artificially, are contrary to that philosophy and to federal and state antitrust laws. Of particular importance is the prohibition on agreements or joint conduct between competitors that harms competition. This includes collaboration with a competitor to decide what to charge for products or other services, or what to pay for services.
- To avoid any implication of an antitrust violation, workforce members should never discuss sensitive business information with a competitor. You should never exchange price information or communicate with a competitor about prices, or anything that may affect prices, or customers. Be particularly careful when attending trade association meetings or other events where interactions with competitors may occur. Antitrust laws are very complex. You should direct any questions about permissible or impermissible conduct to the Office of the General Counsel.

### **Use of Company Assets and Funds**

- You are responsible for ensuring that corporate assets are used for reasonable and bona fide business purposes in accordance with all Company policies. Company assets include not only our equipment, funds and office supplies, but also concepts, business strategies and plans, financial data and other information about Company business. These assets may not be used to derive personal gain for you or for others. You must not transmit Company information to personal emails or unauthorized external parties.

- The Company should not directly or indirectly extend or maintain credit, arrange for the extension of credit, or renew an extension of credit in the form of a personal loan to or for any director or executive officer (or equivalent thereof) of the Company.

### **Prior Criminal Convictions and Delegation of Authority**

- The Company has a legal duty to identify and consider for exclusion from its business operations workforce members whose prior conduct was illegal or inconsistent with the administration of an effective compliance and ethics program. How the illegal activity or other misconduct is related to the specific responsibilities of the individual, as well as how recently the misconduct occurred will be taken into consideration when making hiring, contracting or retention decisions. Workforce members will be subject to periodic background checks and to verification against federal and state debarment and exclusion databases. The Company will not hire, retain, engage or contract with any individual or organization whose name appears on federal or state debarment or exclusion listings, as required. Disclosure requirements under federal and state regulations will be incorporated into applicable vendor, contractor and provider agreements.
- Decisions regarding the hiring or retention of individuals or organizations with histories of felony convictions, other convictions for crimes of fraud, dishonesty or other healthcare crimes, or other reported or discovered misconduct under this corporate policy will be made by the Company's Human Resources department. Issues regarding contracting with any organizations that have felony convictions or other misconduct will be discussed and resolved by the corporate compliance officer.
- The Company will not delegate substantial discretionary authority to individuals whom it knows, or through the exercise of due diligence should have known, have a propensity to engage in inappropriate, improper or illegal conduct.

### **Use of Company E-mail and Internet**

- Internal e-mail systems are acceptable for transmitting confidential data within the enterprise. Workforce members may share protected health information using internal e-mail systems provided the recipient has a business need-to-know and the minimum necessary rule is applied. Our internal electronic mail systems, however, are not secured sources of data transmission and should not be used to send e-mail over the public Internet.
- Messages traversing the Internet are subject to potential public disclosure through innocent misdirection or deliberate intervention if not encrypted. If in doubt, assume that your message will end up on a public bulletin board on the Internet and judge the content and any attachment accordingly.
- When sending sensitive data outside the Company, workforce members must comply with applicable corporate policies, including the Health Information Privacy Policy, Information Security Policy and related Corporate Standards. An encryption option is available to secure messages that are being sent over the Internet. Workforce members can obtain additional information, including instructions, at the Information Technology site on BluesLink. You should contact your leader or check IT4Me on BluesLink with questions related to encrypted e-mail.
- It is a violation of the Code of Business Conduct to create or exchange messages or information on or through the Company's electronic mail systems that is offensive, harassing, obscene, threatening or disparaging to others. Simply stated, do not send anything via the electronic mail systems that you would not want disclosed publicly.

## Records Management

- Workforce members are required to comply with Records Management policies which establish uniform procedures for storing, retaining and destroying corporate records, in accordance with applicable federal, state and local laws. However, in the event of investigations of alleged wrongdoing or as required by court order, destruction of relevant corporate records under the Records Management Policy shall be suspended as necessary and appropriate under the directive of the Office of the General Counsel. You are required to preserve relevant corporate records as directed by the Office of the General Counsel.

## Government Investigations

- If a workforce member is contacted at work or outside of work by a governmental agency concerning a work-related matter, the workforce member should immediately contact his or her leadership, the Office of the General Counsel and Corporate Compliance. Under the law, a workforce member is not required to provide any information to an investigator or agent unless the workforce member has been properly subpoenaed. A workforce member is not under any obligation to speak with an investigator or agent at any time. The Office of the General Counsel can provide assistance in determining how to respond to the request for information. If you do receive a subpoena from a government agency, you should immediately contact the Office of the General Counsel and Corporate Compliance at [ComplianceOffice@bcbsm.com](mailto:ComplianceOffice@bcbsm.com).

## Nondiscrimination in Health Programs and Activities

- Section 1557 of the Patient Protection and Affordable Care Act (ACA) prohibits discrimination on the basis of race, color, national origin, sex, age, or disability in certain health programs and activities. If a workforce member is contacted concerning compliance with this section the workforce member should immediately contact the Company's Office of the Civil Rights Coordinator at [civilrights@bcbsm.com](mailto:civilrights@bcbsm.com). Allegations of noncompliance with this section can also be made by calling 888-605-6461.
- A workforce member is not required to provide any information to an investigator, agent or other person unless the workforce member has been properly subpoenaed. A workforce member is not under any obligation to speak with an investigator, agent or other person at any time.

## Government Programs

- Additional compliance requirements and procedures apply to the Company's participation in government programs.

## Adherence to Fraud, Waste and Abuse Guidelines

- The federal False Claims Act (FCA), as amended by the Fraud Enforcement and Recovery Act of 2009, prohibits anyone from knowingly submitting false or fraudulent claims and from making false or fraudulent records or statements to a recipient of federal funds for payment or reimbursement purposes. The FCA also requires recipients of federal funds to return any overpayment to the federal government. The FCA can be enforced by the Department of Justice, the United States Attorney's Office, or through qui tam actions, where an individual sues on behalf of the government. Violations of the FCA can result in penalties of \$5,500-\$11,000 per false claim submitted; triple the amount of damages suffered by the government, and any applicable attorney's fees and costs.

The FCA includes specific provisions to protect whistle-blowers from retaliation by their employers. Any workforce member, contractor or agent who takes actions to stop an FCA

violation is protected from discharge, demotion, suspension, threats, harassment and discrimination in the terms and conditions of his or her employment relationship if the employer's actions are taken in response to the efforts to stop the FCA violation.

- Pursuant to the federal anti-kickback statute, the Company must not request, solicit, receive, offer, give or make payments of any kind (including bribes, kickbacks and rebates) whether directly or indirectly that would encourage a person to:
  - Refer a person to another person for the furnishing of any item or service covered by a federal program
  - Purchase, lease, order or arrange for any good, facility, service or item for which payment may be made under a government health care program
- Key points of the Company's fraud, waste and abuse program are incorporated into this policy as well as the administrative procedures of the departments involved in detecting and preventing fraud, waste and abuse. It is the responsibility of workforce members to prevent and detect fraud, waste and abuse on behalf of the Company's lines of business.
- The Corporate and Financial Investigations (CFI) department has established a Government Programs Investigative Unit. The mission of this unit is to detect, correct and prevent fraud, waste and abuse as defined by CMS in order to protect the federal and state funds and the Company's corporate assets.

## **How We Solve Ethics Problems**

Some ethical issues we face have clear solutions. Other ethical questions are not so clear-cut, and present us with difficult choices.

The Code of Business Conduct cannot list every potential dilemma. However, it provides guidelines for solving ethical issues.

Here are suggested steps to follow if you are faced with an ethical issue, perhaps because someone has asked you to do something or refrain from doing something that makes you uncomfortable:

1. Understand exactly what you are being asked to do or refrain from doing. Get the facts. Without them, you may be unable to find the best solution to the problem.
2. Clarify your responsibility. Where do you fit in? Are there other responsible parties who should be informed? By bringing the responsible parties together, discussion often leads to a swift, satisfactory resolution of the problem.
3. Ask whether the course of action is fair. If the problem is not a clear-cut matter of law or Company policy, this simple question often serves as a useful guide. If the course of action does not seem fair, why not? Who may be hurt? Is it the Company? Our customers? Other workforce members? Many times the best ethical decision is the one that seems fairest.
4. Ask what is motivating the ethical concern. The motivation for reporting an ethical matter must never be to retaliate against or embarrass another person, especially another workforce member. The ethical consideration and reporting process is to be used to help maintain high ethical standards and full compliance with the law.
5. Whenever possible, discuss the problem with your leadership. This advice is basic to most situations and should be considered as you proceed through the above steps. Your leadership is responsible for helping you solve problems. In most cases, your leadership

will have a broader Company perspective and will appreciate being brought into the decision-making process early.

6. If it is inappropriate to discuss the issue with your immediate leadership first, you may raise the issue directly with Corporate Compliance at [ComplianceOffice@bcbsm.com](mailto:ComplianceOffice@bcbsm.com), or with the Corporate Compliance Officer, the General Counsel, the vice president of Corporate Compliance, the executive vice president of Operations and Business Performance, or the vice president of Human Resources. In an exceptional situation, an issue may be raised with the chair of the Audit Committee of the boards of directors. Email [ComplianceOffice@bcbsm.com](mailto:ComplianceOffice@bcbsm.com) for current contact information.

Issues related to conduct of members of the board or director selection councils may be raised as provided above or to the Nominating and Governance Committee of the BCBSM board. The Nominating and Governance Committee of the board will consider and decide issues related to board and council member conduct.

For general compliance questions and concerns, contact the Corporate Compliance at [ComplianceOffice@bcbsm.com](mailto:ComplianceOffice@bcbsm.com)

In addition, you may call the Company anti-fraud hotline at 800-482-3787, where the information may be shared anonymously if you choose. Issues may also be forwarded electronically to [CFIfraudinquiries@bcbsm.com](mailto:CFIfraudinquiries@bcbsm.com)

Privacy questions or concerns should be sent to the Privacy mailbox at [Privacy@bcbsm.com](mailto:Privacy@bcbsm.com)

Issues related to Medicare business should be reported on our Medicare anti-fraud hotline at 888-650-8136 or TTY800-588-2711.

Issues related to possible Medicare fraud may be reported to the Health and Human Services Office of the Inspector General at 800-447-8477 or TTY 800-377-4950.

## **How We Respond to Inquiries and Reports Involving the Code of Business Conduct and Compliance Issues**

The Company is committed to creating a work environment where inquiries and reports involving the Code of Business Conduct, suspected violations of federal or state law, suspected fraud, waste or abuse or other compliance issues are encouraged and accepted. Anyone may report a compliance issue or incident, using the options listed above. Reports may be made confidentially or anonymously. You should feel free to raise ethical concerns in good faith without fear of retaliation.

We will review reported potential violations and investigate as appropriate. If criminal conduct is confirmed, our response may include actions to mitigate any harm caused. Mitigating actions could include making appropriate restitutions and assessing the Company's compliance program to ensure the program is effective and consistent with applicable regulations.

We encourage you to think about ethical issues, report problems or concerns and ensure your

behavior conforms to the standards in the Code.

If you are involved in reported potential violation, you will be treated fairly and given an opportunity to explain your actions.

Since you are encouraged to act as a good corporate citizen and raise issues about questionable activities, negative actions will not be taken against you for making a complaint or disclosing information about an activity that you believe in good faith may violate this Code or any laws, even if your belief is mistaken. Anyone who attempts to retaliate against you for reporting problems or concerns will be disciplined.

Please note that known or suspected violations of the Corporate Ethics and Compliance Policy or any laws need to be reported. You are obligated to immediately report instances of potential misconduct or non-compliance. You are required to participate in internal and external investigations of perceived wrongdoing. Failure to report or cooperate in an investigation will subject you to discipline, including possible termination of employment.

Remember that when you make an inquiry or report, it will be handled as confidentially and discreetly as possible. We may, however, be required to substantiate any allegations of wrongdoing. A written record of your inquiry and our response will be made and forwarded to the vice president of Human Resources or the vice president of Corporate and Financial Investigations (if related to fraud) for review and follow-up as required.