BlueCross BlueShield of Alabama

Code of Ethics and Business Conduct

OCTOBER 2026



Please contact the Compliance Office with any questions regarding the Code of Ethics and Business Conduct. Listed below are available resources.

How You Can Contact Compliance:

Compliance Help Line 1-877-988-9823
HIPAA Privacy Help Line..... 1-877-668-7222
Fraud Help Line 1-800-824-4391
Fax Line (for Fraud, Compliance, and HIPAA reporting) 205-220-2984
Compliance Email ..... ComplianceOffice@bcbsal.org
HIPAA Privacy Email..... HIPAAPrivacy@bcbsal.org
HIPAA Security Email ..... HIPAA-Security@bcbsal.org
Fraud Email ..... Fraud@bcbsal.org
Anonymous Online Compliance and HIPAA Reporting . ReportToCompliance.com

When you call the Compliance or HIPAA Help Line or report online, you have the option of identifying yourself or remaining anonymous.

How to get answers to your questions about the Code of Ethics and Business Conduct

Blue Cross and Blue Shield of Alabama has contracted with an independent third party to receive all calls to our Compliance and HIPAA Help Lines, as well as online reports. Convercent, the independent third party, will protect the identity of those making reports of noncompliance subject to applicable law, regulation or legal proceedings.

When you call the Compliance or HIPAA Help Line or report online, you have the option of identifying yourself or remaining anonymous. If you choose to remain anonymous, please provide enough information about the incident or situation to allow a thorough investigation.

Cover photo by Brian DeMarco

INTRODUCTION



A Letter from Our CEO

Dear Associate,

Since 1936, our Company has developed a solid reputation reflecting trust and steadfast values. Because integrity is fundamental to the way we do business, we are a respected name and a healthcare leader in Alabama and beyond. Our ethical practices have helped us build a strong foundation and are one of the reasons our customers know they can depend on us when it matters most.

It is important to remember that the ends do not justify the means. We must ensure we know and follow the correct path of making ethical decisions because holding true to our principles and values is critical to our success. This is just good business sense for a successful future.

Our Code of Ethics and Business Conduct, also referred to as the Codebook, provides our workforce clear direction on expected ethical behavior. It is our playbook that ensures we act with integrity and honor - on behalf of the Company. I encourage you to familiarize yourself with our Codebook and the principles that guide our organization.

If you have any questions about proper conduct or the Compliance Program, please contact your manager or the Compliance Office.

With your commitment, we can ensure Blue Cross and Blue Shield of Alabama continues to do the right thing, at the right time, and for the right reason.

Sincerely,

Tim Vines
President and Chief Executive Officer

Making ethical decisions is just good business sense for a successful future.

TABLE OF CONTENTS

It's your responsibility to ...

- KNOW THE RULES 2
- BE AWARE AND REPORT VIOLATIONS 4
- RESPECT OTHERS 8
- KEEP IT CONFIDENTIAL 9
- AVOID CONFLICTS OF INTEREST 13
- KEEP ACCURATE RECORDS 18
- USE COMPANY RESOURCES WISELY 19
- PROPERLY REPRESENT THE COMPANY 21
- WORK SUCCESSFULLY WITH OUTSIDE ENTITIES . . . 22
- WORK APPROPRIATELY WITH GOVERNMENT 24
- UNDERSTAND SPECIAL RESPONSIBILITIES 26
- APPENDICES 28

OUR CORPORATE VALUES

Respect Our Customers

Achieve Excellence

Retain Financial Strength

Realize Full Potential

Pursue Knowledge

Act with Integrity

Give Back to the Community

Compliance Program

The purpose of our Company's Compliance Program is to set standards for conduct through the Code of Ethics and Business Conduct (the "Codebook") and encourage ethical behavior through education and training. Our Company's Compliance Program offers ways to report unethical behavior and ask questions about compliance issues. It also includes procedures for detecting and investigating unethical behavior. We continually aim for improvements in our practices, policies and environment to make the Compliance Program as effective as possible.

Codebook

Our Codebook describes the standards and rules that not only associates – but Company managers, officers and directors – must follow. These standards and rules are based on our Corporate Values of "Act with Integrity" and "Respect Our Customers," as well as state and federal laws. This Codebook includes statements of Company policies that are the backbone of the Code of Ethics and Business Conduct. In addition, the complete set of Company policies is available under Corporate Operating Policies ("COP") on Web01. Individual departments also have policies and procedures that can be found on the Documentation Online Reference System (DORS) or within your department or division.

You are responsible for knowing these policies and procedures and the Codebook. Your knowledge of these rules and standards protects you and the Company.

Our Codebook is also provided annually to our First Tier, Downstream, and Related Entities (FDRs) and vendors. For more information, see the *Work Successfully with Business Associates* section later in this booklet.

Annual Training

You are required to complete annual Compliance training; Fraud, Waste and Abuse training; as well as any specialized training in your department or area. You must review and be familiar with the Codebook and abide by it. The online Codebook Acknowledgement Form on the Compliance and Ethics website and the training transcript in the *HUB* are methods used to ensure associates become familiar with the information in the Code of Ethics and Business Conduct.

Laws and Regulations

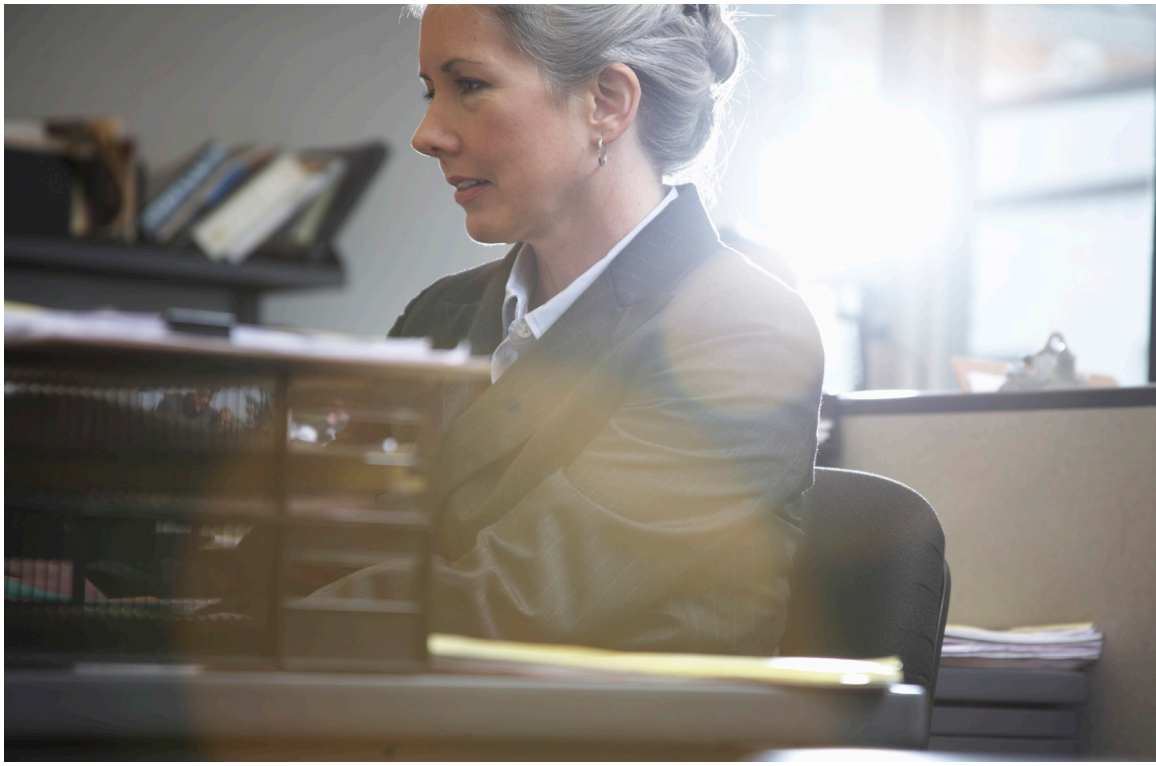
One of the purposes of our Compliance Program is to educate associates about our obligations under the law. Our Company is subject to a variety of laws and regulations that address requirements such as licensure, accuracy in records, confidentiality concerns, Medicare, the Federal Employee Program, healthcare reform requirements, as well as other federal or state programs. Therefore, we all must be knowledgeable about and comply with the laws and regulations that apply to our lines of business. See Appendix C for examples of such laws and regulations.

Table of Contents

Corporate Operating Policies

Policies that apply to all associates are available on WEB01. The policies cover a wide range of topics, and you are responsible for knowing them and acknowledging them annually. The policies range from HIPAA policies to Information Security policies to Human Resources policies.

Know and follow the laws, policies and procedures that pertain to your job.



BE AWARE AND REPORT VIOLATIONS

How You Can Contact Compliance

Compliance Toll-free Help Line:
1-877-988-9823

Fax Line (for Fraud, Compliance, and HIPAA reporting):
205-220-2984

HIPAA Privacy Toll-free Help Line:
1-877-668-7222

Compliance Email:
ComplianceOffice@bcbsal.org

Anonymous Online Compliance and HIPAA Reporting:
ReportToCompliance.com

You may also contact any Compliance Office staff member including the Compliance Officer.

Each Compliance staff member, along with contact information, is listed on the Compliance website available through Web01.

Your Duty to Report Violations and Cooperate in Ethics Investigations

You have the duty to:

- Report any violations of the Code of Ethics and Business Conduct – even suspected or potential violations – to the Compliance Office, your manager or department head;
- Participate in compliance investigations; and
- Cooperate with compliance investigators.

You may report anonymously. If you report using your name, the Compliance Office will keep your identity confidential, unless disclosure is necessary to resolve your reported issue, or disclosure is required under the law.

The Company is committed to establishing an environment that encourages and allows associates to seek and receive prompt guidance before engaging in conduct that may violate the Codebook or any local, state or federal law, rule or regulation.

Your Duty to Report Healthcare Fraud

Healthcare fraud is an intentional deception, concealment or misrepresentation by an individual or entity, knowing the misrepresentation could bring some benefit to them or another party they are not legally entitled to receive. All associates are responsible for protecting the honest administration of our customers' benefits.

You must report all suspected healthcare fraud activity to the Compliance Office or Network Integrity. If you suspect that a provider, subscriber or group is committing healthcare or pharmacy fraud and abuse:

- Call the Fraud Help Line at 1-800-824-4391;
- Send an email to "Fraud" (Fraud@bcbsal.org); or
- Visit **AlabamaBlue.com**, and click on "Fraud & Abuse" at the bottom of the page.

If you are asked to provide information as part of an investigation, you have a duty to provide prompt, complete, accurate and truthful responses. Providing false, inaccurate or misleading information in response to an investigation or inquiry could be considered a Compliance violation.

You May Not Retaliate

Blue Cross and Blue Shield of Alabama has a strict non-retaliation policy. The Company, its associates, managers, officers and directors may not retaliate or discriminate against you for reporting noncompliant behavior or healthcare fraud. This is also true when you cooperate in an investigation, even if it turns out that no actual noncompliant behavior took place. If you feel that you are being retaliated against because of a report you made, report it to Compliance immediately.

If you are the subject of a compliance investigation, you must not try to find out who made the report to Compliance - or retaliate in any way against anyone within the Company or outside of the Company. Doing so may result in disciplinary action, up to and including termination.

Questions and Answers

What should I report to the Compliance Office?

If your concern falls into any of the following areas, you should contact the Compliance Office:

- Violation of a government standard or regulation;
- Violation of local, state or federal laws that are not employment-related;
- Conflict of interest;
- Acceptance/offer of gifts (and/or) entertainment from outside sources;
- Associate fraud;
- Improper disclosure of proprietary or confidential information;
- Accounting, auditing and internal control irregularities;
- Retaliation for reporting a compliance issue;
- Falsification of reports, records or files;
- Theft;
- Any other violation of the Code of Ethics and Business Conduct; and
- Improper access, use or disclosure of member information.

What information should I provide when I email or call Compliance?

The following are general guidelines for the kind of information that you should provide when reporting a compliance issue or making an inquiry:

- Describe the situation and department, business area, etc.;
- Identify approximate dates when events occurred and names of persons involved;
- Indicate whether you know about the circumstances from your direct observation or whether someone told you about it;
- Describe how the situation and events occurred;
- Describe any relevant documents or documentation and where they are located.

If you report anonymously, report enough information to allow Compliance to investigate. If you report through the Compliance or HIPAA Help Line or through the online reporting website, ReportToCompliance.com, you will be issued an access code so you can provide additional information as well as receive updates anonymously.

What should I do if I suspect a Compliance violation has occurred?

Report any violation or suspected violation of the Code of Ethics and Business Conduct to the Compliance Office or your manager. You can also contact the Compliance (1-877-988-9823) or HIPAA (1-877-668-7222) Help Line or visit ReportToCompliance.com to report online.

BE AWARE AND REPORT VIOLATIONS

What happens when Compliance receives a report or inquiry?

The Compliance Office will review all reports received of suspected violations of the Code of Ethics and Business Conduct.

If the matter reported is not a potential compliance violation but is a Human Resources, Network Integrity or other matter, Compliance will refer the matter to the appropriate area.

If there is a suspected violation of our Code of Ethics and Business Conduct, the Compliance Office will conduct an investigation. Investigations require in-depth research and may also involve the assistance of other departments including Human Resources, Internal Audit, Information Security, Technology Support, Network Integrity and Legal.

If you report using your name, the Compliance Office will keep your identity confidential, unless disclosure is necessary to resolve what you reported or disclosure is required under the law. In such cases, disclosure will be limited to only those individuals within the Company necessary to address the issue. After the investigations are completed, appropriate corrective actions are taken as needed.

If you are asked to cooperate in an investigation, you must provide prompt, true, accurate and complete information. Failure to do so could be considered a compliance violation.

Your co-worker makes jokes about another co-worker's race and religion. Is that OK?

No. This behavior is inconsistent with our Company's standards and expectations. You should ask your manager or an Associate Services representative to address the situation.

If I report what I think is a violation of the Code of Ethics and Business Conduct, and no violation is found upon investigation, will I get in trouble?

No. There will be no action taken against you for reporting a suspected violation.

If there is a suspected violation of our Code of Ethics and Business Conduct, the Compliance Office will conduct an investigation.

What factors are considered in determining consequences for compliance violations?

The Compliance Officer may take into account the following factors in determining the appropriate disciplinary action for a violation of the Code of Ethics and Business Conduct or related policies and procedures:

- The nature of the violation and the effects on the Company and its clients and members;
- The involvement of the associate in the violation, either directly or indirectly;
- Whether the violation was willful or unintentional;
- Whether the violation represented an isolated occurrence or a pattern of conduct;
- Whether the associate in question reported the violation;
- The degree to which the associate cooperated with the Company's investigation and fully and truthfully responded to questions;
- If the violation was the failure to supervise another associate who violated the Code of Ethics and Business Conduct (or related policies and procedures), the degree of the failure and lack of supervision;
- The disciplinary action previously imposed for similar violations; and
- The associate's past violations.

The Company will document the reasons supporting disciplinary actions taken for violations of the Code of Ethics and Business Conduct (and related policies and procedures).



RESPECT OTHERS

Respect in the Work Environment

Each of us has the right to work in an environment free of harassment or discrimination because of race, sex, creed, national origin, etc. We have an obligation to treat each other with courtesy and fairness and respect the dignity of others. Federal and state laws prohibit discrimination, sexual harassment, and similar misconduct. Reporting an actual or suspected violation of this policy will not subject the reporting associate to any retaliation. However, if the reporting associate took part in the harassing or discriminatory behavior, the associate would still be subject to the Company's policies and procedures. Self-reporting will not absolve you of the consequences of inappropriate actions.

Respect Our Customers

We respect our customers and never forget they come to us by choice. We listen to our customers, work to understand their needs, and partner with them to do what is in their best interest.

Drug-Free Workplace (Drugs and Alcohol)

You may not possess, use, or sell illegal or controlled substances on Company property. You may not work under the influence of illegal or controlled substances or alcohol (whether or not you are legally intoxicated). This kind of behavior may be considered an intolerable offense. An intolerable offense will result in termination and may be reported to law enforcement.



HIPAA Privacy

You must keep our members' information private and confidential. This is our ethical obligation and the law under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Any information we gather and maintain on our members is confidential and considered protected health information (PHI). **Remember these three rules:**

1. **You may only access the minimum amount of information needed to do your job.** If you obtain access to or use member information that is not needed to do your job, you violate the Company's HIPAA policies. This is true even if you gain access to your own contract information or that of family members, or if you only access member information that is not "health information" such as an address or birthday.
2. **You may only disclose information to others – including other associates – when they have a legitimate business need to know.**
3. **Blue Cross and Blue Shield of Alabama associate PHI is PHI under HIPAA and should be handled with extreme care. Your fellow associates are members too.**

If you disclose member information to another person without a legitimate business need to know, you have violated the Company's HIPAA policies. This includes disclosing more information than the other person had a legitimate need to know.

If you violate the Company's HIPAA policies, you could be subject to disciplinary action. You may also be subject to federal or state prosecution.

HIPAA Security

The security portion of HIPAA focuses on securing sensitive information in electronic formats. Our HIPAA security policies help you protect information while performing your daily work responsibilities. Whether you are a database administrator (determining how to store sensitive information) or a customer service associate (needing to send a member account information), you can find direction in these policies on how to accomplish these tasks securely. You are responsible for knowing and abiding by our HIPAA Privacy and Security policies as you fulfill your job requirements each day.

Proprietary Information, Trade Secrets, and Confidential Information

You are responsible for guarding and keeping confidential the Company's trade secrets and proprietary and confidential information. This is information that is not usually made public and would be useful to competitors.

Common examples include: financial data, plans for new projects and products, lists of suppliers and customers, contracting arrangements, wage and salary data, changes in management, and systems and business processing methods.

Within the Company, you can only discuss Company trade secrets and proprietary and confidential information with other associates on a need-to-know basis.

Outside the Company, you can only disclose proprietary or confidential information if confidentiality agreements have been arranged through the Legal Department with the individual or organization to whom you are making the disclosure.

You can only discuss or disclose member/customer information outside the Company when expressly allowed under HIPAA. Within the Company, you can discuss member/customer information only with those associates who have a business need to know. This obligation continues even if you leave the Company.

What are examples of proprietary information, trade secrets and confidential information?

- Any information covered by HIPAA Privacy Rules;
- Provider data such as NPIs and tax ID numbers;
- Information concerning diagnosis or procedure codes;
- Home phone numbers and addresses of subscribers or beneficiaries;
- Bank account information or credit card numbers;
- Company financial data;
- Intellectual property, trade secrets and proprietary information including Company research; and
- Company training and marketing materials.

Examples of misuse of proprietary information, trade secrets, and confidential information include the following:

- Viewing information that you do not have a business need to look up;
- Discussing a claim with a business associate who is not involved in the adjudication of that claim;
- Showing others pre- and post-operative photos or information;
- Disclosing any information where there is no business need to know;
- Looking up your own information or that of relatives, ex-relatives, or any other beneficiaries or subscribers without a business reason;
- Processing claims for relatives or former relatives with or without permission;
- Sharing Company intellectual property, trade secrets and marketing materials outside the Company;
- Discussing Company trade secrets and corporate strategy with competitors; and
- Sharing Company financial and audit reports outside the Company or with those who have no business need to know.

Questions and Answers

Is it a violation of the Company's HIPAA Privacy policies for me to access my own contract using the claims system?

Yes. You should only access PHI for reasons directly related to your job duties. If you have a question about your own contract, you should call the customer service number on the back of your insurance card or access your account using the *my*BlueCross tab on **AlabamaBlue.com**.

What if I want to look up information about my children's contracts and claims?

You cannot look up information on your children's accounts through your job-related system access. You are permitted to obtain this information only through *my*BlueCross, or by calling the customer service number on the back of your card.

What if I only use my system access to look up a member's birthday or address?

You may not use your system access to look up any member information unless you have a business need to do so. This includes information such as an address or birthday.

If I become aware of an unauthorized disclosure of PHI, what should I do?

You must immediately notify your DiPR. Your DiPR will then be able to take proper steps to mitigate the situation. If your DiPR is not available, email the HIPAA Privacy Office.

What should I do if my laptop is lost or stolen on a weekend or after business hours?

In case of a lost or stolen laptop, mobile device, USB, SecureID token or any other Company equipment, immediately call the Corporate Support Center at 205-444-5442 or 1-877-282-4000 and follow the voice prompts to be connected to the Information Security Incident Response Line. If no one is available to take your call, leave a detailed message. An alert will be sent to the Incident Management Response team on call. A team member will respond to your message.

KEEP IT CONFIDENTIAL

My job requires me to send sensitive information to people outside the Company. How can I send this information securely?

First, verify that the recipient is authorized to receive the information. Second, confirm their email address or fax number. If you are sending the information via email, make sure the email is sent securely by either typing #secure# in the subject line after your subject, or by clicking the Encrypt key button on your email toolbar. If you are sending the information via fax, include the fax cover sheet with our Company confidentiality disclosure and call the recipient to verify receipt.

Is it OK to leave PHI out on my desk or on the printer when I leave for the day or for an extended period?

No. Whether you are working in the office or remotely, you should not leave PHI on your desk, the printer, a fax machine or in other unsecured areas for an extended period of time, including when you complete work for the day. Instead, PHI should be stored securely and out of sight.

Is it OK to use Company assets such as work time, printers, email, internet, etc., to support a second job?

No. This behavior is inconsistent with our Company's standards and expectations.



What is a Conflict of Interest?

A conflict of interest is when your own interest or involvement in a financial or personal matter could get in the way of your obligation to the Company. Conflicts of interest include:

Private Financial Gain When your private financial interests could influence your decisions or actions in your job or role with the Company. Such interests might include the following:

- Your personal interest or a family member's interest in an enterprise that has a business relationship with the Company. This restriction does not apply to minimal holdings of stock or other securities of a corporation whose shares are publicly traded, and which may incidentally do business with the Company.
- Your investment or a family member's investment or participation in another business that competes directly with the Company. This does not apply if the investment is not a significant part of your or your family's income or net worth, or the area of competition has minimal effect on the Company.

Second Job or Outside Activity When your second job or outside activity could conflict with your job or your obligation to the Company or hurt the Company's reputation in the community. Such conflicts may include:

- A second job conflicts with your job with the Company when it results in your failure to meet goals, inability to perform job duties, tardiness, absenteeism, sleeping on the job, or inability to work required overtime. If you have a second job in the healthcare industry, your employment should not include the review of cases or the coding or submission of claims. Remember that any second job must be reported to Compliance on a Conflict of Interest statement as described in the section below.
- Outside activities should not be performed during your work time because they could interfere with your regular duties and affect the quality and quantity of your work. Working on an outside activity during your work time could also negatively affect the Company's reputation.

What are examples of employment positions that could present a conflict of interest?

Some examples of employment positions that conflict with the Company include:

- Associates who work in positions keying, reviewing or otherwise dealing with claims information for any healthcare provider who conducts business with the Company.
- Individuals who audit, review and investigate providers or other entities that deal with confidential or proprietary information who also work in a position in which the associate or the associate's immediate family could be required or expected to take an adversarial position against the Company.
- Outside positions that cause associates to arrive late or leave early.
- Any outside position that prevents associates from performing their job with the Company, including not being able to work required overtime.
- Selling products or services that compete with the Company's products or services.

Prohibition on Personal Loans

To avoid a real or perceived conflict of interest, the Company shall not extend credit or arrange for the extension of credit in the form of a personal loan for any director, officer, manager or associate of the Company (except for travel advances).

When you have a question about a possible conflict of interest

If you think you may have a possible conflict of interest due to your second job, outside activities or investments, contact the Compliance Office.

Note to Health Professionals

Health professionals in the Company may be asked to review medical information about a member they have encountered in their roles outside the Company (for example, as a nurse or pharmacist working in a hospital or as a physician in private practice). In this situation, the health professional should give the review to their manager or another health professional in the department and follow any other departmental procedures to avoid any conflict.

Conflict of Interest Statement

You must complete a Conflict of Interest statement when you are first hired and again each year. You are required to complete a new Conflict of Interest statement when any information on your previous Conflict of Interest statement changes. Your Conflict of Interest statement is reviewed by the Compliance Office. The Compliance Office will make every effort to mitigate an actual or potential conflict. If you have a conflict that cannot be mitigated by the Compliance Office, you will be asked to change your situation so that you do not have a conflict. Keep in mind that the Conflict of Interest statement is an official Company document and that you are required to complete it accurately. The Company will maintain the information you provide on your Conflict of Interest Statement in confidence, unless disclosure is necessary to address your potential conflict. In such cases, disclosure will be limited to only those individuals within the Company necessary to address the conflict.

Violent Crime Control and Law Enforcement Act

Federal laws prohibit an individual who has been convicted of certain crimes from involvement or employment with an insurance company, and from providing services to government programs such as Medicare. For that reason, when you are hired, and at any time during your employment, you must disclose on your Conflict of Interest statement any misdemeanor or felony convictions, or any instance when you admitted guilt, pled no contest, or nolo contendere to a crime or dishonest act.

What are examples of acceptable and unacceptable gifts?

Acceptable Gifts

- Flowers
- Gift baskets
- Fruit baskets
- Plants
- Candy
- Paperweight
- Letter Opener
- Picture Frame
- Book
- Calendar
- Mug
- Key chain
- Balloons

Unacceptable Gifts

- Cash, checks, gift certificates or gift cards
- Expensive leather goods
- Premium seats at sporting or theater events
- Use of a vacation home
- Jewelry
- Free trip
- Free hotel rooms
- Airfare
- Expensive clothes
- Television set
- CD player/MP3 player
- iPod/iPad
- Laptop computer

Information you disclose will be reviewed and considered on a case-by-case basis. Any employment decisions will depend upon factors such as the nature and seriousness of the crime and the nature of the associate's job.

As an insurance company, Blue Cross and Blue Shield of Alabama must complete criminal reinvestigations for all associates at least once every five years, and such reinvestigations are considered terms of employment with the Company.

Any criminal convictions that the Company becomes aware of during the criminal reinvestigation process will be compared to the associate's Conflict of Interest statement. An untrue answer or omission of pertinent information on the Conflict of Interest statement could be considered falsification of a Company record or document.

Accepting Gifts, Gratuities, including Travel and Entertainment Expenses and Honoraria

In your position with the Company:

- **You may not ask for or solicit a gift or favor** including a meal, entertainment, special treatment or payment of expenses from any external person or organization.
- **You may never accept a gift of cash or a cash equivalent** such as a gift card from a source outside the Company.
- **You may accept small non-cash gifts of nominal value.** A gift is considered to be of nominal value if its value does not exceed $100. During a year (any 12-month period), the total value of gifts received from any one source cannot be more than $200. The gift must be received in the ordinary course of a business relationship.
- **You must not accept travel expenses, registration fees or honoraria** from vendors, trade groups or professional associations. If you do not believe the organization sponsoring an event you are planning to attend falls into one of those categories, contact the Compliance Office. Remember the general rule: if it is important enough for you to attend a meeting or conference, then it should be paid for by Blue Cross.
- **You should never accept anything of value in situations where the transaction could be viewed as being improper.**
- When you return or refuse gifts or offers of travel expenses or honoraria, you should **send a letter stating you cannot accept the gift or offer due to our Company's policy**. You should also send a copy of your letter to the Corporate Compliance Office where it will be kept on file.

The templates for the appropriate letters are located on the Compliance website, as well as Appendices A and B at the end of this Codebook.

If you have questions about accepting a gift, contact the Compliance Office.

Accepting Items from Random or Blind Drawings

You may participate in random or blind drawings, such as for door prizes, at conferences or professional meetings, unless accepting the prize could be viewed as improper. Random drawings do not fall under the gift policy provided the drawing is truly random, and there is no expectation you or the Company will give anything in return for the prize.

Giving Gifts or Business Courtesies

Our Company believes business should be won or lost based on the merits of our products and the record of our performance. We can offer business courtesies – small gifts or favors that are reasonable in nature and amount – in the course of business relationships. Examples of business courtesies are meals, drinks, entertainment, hospitality, recreation, door prizes, transportation, tickets, passes or promotional items. Business courtesies should never be extended to customers under circumstances that might create even the appearance of impropriety.

Our Company believes business should be won or lost based on the merits of our products and the record of our performance.

Special Rules for Giving Gifts

Gifts or Business Courtesies to Government Officials: State and Federal Ethics Laws addressing government relations and gifts to government officials are strict and generally include potential prison terms and extensive fines. While these laws do allow for business courtesies in certain very limited situations, the rules are complex and change frequently.

Those associates within the Company who work in the Government Relations Department are abreast of these complex rules and attest that their actions on behalf of the Company are in accordance with applicable requirements of Title 36 of the Alabama Code, as well as applicable Federal laws and rules.

All other associates are prohibited from offering or giving anything of value to any government official, government employee or their contractor, or accepting anything of value from those individuals without first obtaining an approved waiver from the Compliance Officer.

Gifts or Business Courtesies to current or prospective Medicare Members (Part C or Part D): There are special marketing rules for Medicare Advantage and Medicare Part D. Consult the guidelines or check with your manager to be sure you are following these rules.

Gifts or Business Courtesies to Unions: We must report any gifts, entertainment or other items of value we give to unions, union officials, union employees or other union representatives. This is required by the Labor Management Reporting and Disclosure Act (LMRDA), under which the Company must report items of value given or paid to unions to the Labor Department. The law provides a limited exception when these items total less than $250 annually. Contact Vendor Payment Services or the Compliance Office for guidance if your position requires interaction with unions or union officials.

Questions and Answers

When should I fill out a Conflict of Interest statement?

You should complete a Conflict of Interest statement at least once a year when the Compliance Office asks everyone to fill out a new form. Also, you should fill out a new form any time information on your previous conflict of interest statement changes. To get a new form, contact the Compliance Office.

I was recently convicted of a DUI. Does this conviction need to be disclosed on my Conflict of Interest form?

Yes. You are required to disclose any misdemeanor or felony criminal convictions. The Company conducts criminal background checks on all associates at least every five years. If the criminal background check does not match what was reported on your Conflict of Interest form, then this could be considered falsification of Company records.

What should I do if I receive a $5 Starbucks gift card from a vendor?

The Starbucks gift card is an unacceptable gift because gift certificates and gift cards are considered cash equivalents (the same as cash). Gifts of cash and cash equivalents from outside sources are always unacceptable regardless of the dollar amount. The gift certificate should be returned to the vendor. There is a return gift letter located on the Compliance website to assist you.

I am planning to attend an upcoming conference, and a vendor has offered to pay for my registration fees, hotel and travel expenses. Can I accept the payment?

No. You should not accept payment from a vendor for registration fees, hotel stays or travel expenses.



KEEP ACCURATE RECORDS

Our Company relies on associates to keep accurate and honest books, documents and records. You must check and double check the information you gather and put on paper or enter electronically. You must never falsify books, documents or records – or even intentionally mislead by knowingly omitting information. Even backdating a report or form can be falsification.

Remember, this rule applies to books, documents and records you create for or on behalf of the Company, as well as those you submit to the Company, whether verbally, on paper or electronically. Providing false, misleading or inaccurate information as part of a Company investigation can be a violation of this rule. Even backdating a report or form can be considered falsification.

What are examples of Company books, documents and records?

- Financial and accounting records
- Spreadsheets
- Job applications and resumes
- Time sheets
- Doctors' excuses
- Tuition reimbursement forms
- Applications for hardship withdrawals and loans from your 401(k) plan
- Expense records
- Information submitted to a government agency or the Blue Cross and Blue Shield Association

Retention of Records

You may not discard or dispose of Company records that must be kept by law, or because the Company requires the records be kept. Examples of records that must be kept for certain periods are tax and financial records, contracts, health information, records related to Medicare or our Qualified Health Plans, and personnel records.

Improper Influence on Conduct of Audit

No associate of the Company, its affiliates, directors, officers, managers or any other person acting under their direction, shall take any action to fraudulently influence, coerce, manipulate or mislead anyone engaged in the performance of an audit of the Company.

Costs That are Not Allowable

Our Company policy states costs that are expressly not allowable for reimbursement from the government, and costs for which there is no good faith basis, will be identified and accounted for as not allowable costs. Reimbursement from the Federal Government will only be requested for those costs allowable in accordance with laws and regulations.

You must never falsify books, documents or records… even backdating a report or form can be falsification.

Use of Company Funds and Assets

Each of us has the responsibility to protect Company assets and funds. Our primary use of Company assets and funds must be for Company business.

We are permitted to use our telephones, office computers and Company email for personal reasons on a limited basis (for example, making doctor appointments, checking on children or parents, or checking your bank account).

However, Company assets, including your work time, should never be used to support a business other than Blue Cross and Blue Shield of Alabama or for personal financial gain.

Personal use of Company assets is a privilege, and you must follow your manager's or department's guidance concerning use of Company assets.

Your personal use of email or internet must not interfere with doing your job or with other associates doing their jobs. Your personal use must never result in excessive cost to the Company.

Your use of Company email must never harm the Company's reputation. You should not send personal emails that include your Company title, department, the Company name or Company logos. Providing this information may give the impression you are speaking on behalf of the Company when you are actually expressing your personal opinions or the opinions of others.

Remember that Company equipment and electronic services provided by the Company, such as internet, email and telephone systems, are Company property. Therefore, you should have no expectation of privacy when you use them. Associates are not permitted to send or forward chain letters or chain emails.

You are responsible for assuring that Company assets, including the Company's communication networks, are used primarily for legitimate Company business purposes. Personal use of these assets is permitted as long as the frequency and cost are not excessive, and the personal use does not interfere with Company business or an associate's work.

However, Company assets should never be used to support a business other than Blue Cross and Blue Shield of Alabama or for personal financial gain. Any questions regarding limited personal use should be directed to your manager or the Compliance Office.

Remember – just because a website is not blocked does not mean the Company would condone your visit to that site, and just because the filter does not stop a message does not mean that the Company condones its language or content. It is your responsibility to conduct your activities within published guidelines.

What are examples of Company assets?

This list might prompt you to consider things that could be considered Company assets. It is NOT an all-inclusive list.

- Business concepts
- Business strategies and plans
- Corporate funds
- Intellectual property
- Corporate credit card
- Customer lists
- Associate names
- Email
- Fax machines
- Financial data
- Internet access
- Personal computers
- Office equipment
- Office supplies
- Telephones
- Company-issued cell phones
- Copy machines
- Scanners
- Data storage devices
- Associate work time

USE COMPANY RESOURCES WISELY

Examples of limited personal use of Company assets include the following:

- Providing your child's teacher with your work email address for emergencies or communications during the work day;
- Checking the weather;
- Periodically checking in with relatives;
- Faxing a limited number of documents to your child's school, a doctor's office or bank;
- Calling doctors and dentists to schedule personal appointments;
- Confirming lunch plans with friends and relatives;
- Providing your family with your work phone number or email address;
- Checking grades or assignments online;
- Checking and managing your 401(k) account;
- Checking balances (for example, bank or credit card accounts); and
- Limited electronic banking.

Some examples of inappropriate personal use include:

- Any use of corporate assets for personal financial gain;
- Excessive use (that is, if more than a limited amount of personal use of the asset occurs). Your manager can help you determine if your use is excessive;
- Time spent sending or receiving personal email that exceeds more than just a few minutes per day;
- Use of profanity in email;
- Use of email to ask or solicit others to take a particular action which is not related to your job;
- Sending or forwarding chain emails;
- Use of email to create a hostile work environment or to harass others;
- Use of email to promote your political or religious opinions or opinions of others;
- Use of email to take political polls or surveys;
- Saving images on Company assets that depict nudity, pornography or sexually explicit images and/or forwarding such images through email;
- Accessing and communicating in external chat rooms;
- Accessing sexually explicit or inappropriate websites;
- Use of the internet to access personal email through systems other than Outlook (for example, AOL, Hotmail, Yahoo and Gmail);
- Accepting collect calls.

We are permitted to use our telephones, office computers and Company email for personal reasons on a limited basis.



When does inappropriate use of Company assets become "Occupational Fraud"?

When an individual uses their job or occupation for personal enrichment through deliberate use or misappropriation of the assets or resources of the organization that employs them, that is occupational fraud, as defined by the Association of Certified Fraud Examiners (ACFE).

Examples of occupational fraud are not only the obvious ones - theft or embezzlement or taking a kickback from a vendor - but also such examples as:

- Wrongfully charging travel or other expenses to the company
- Falsifying information on reports provided to regulatory agencies

Such actions may result in disciplinary action, up to and including termination.

Social Networking and Media

Social Networking, media sites, personal websites and blogs are widely used in our culture. The Company respects the right of associates to use these platforms during their personal time. You should consider the following basic rules before posting information online:

- You are personally responsible for anything you post online and liable for postings found to be defamatory, harassing, or in violation of any federal or state law.
- Your online postings may not violate the Code of Ethics and Business Conduct or any Corporate Operating Policy. For example, you must maintain confidentiality of member information as well as Company proprietary information.
- Care should always be taken when you are online to ensure you aren't giving anyone the impression when you are online that you are posting information on behalf of the Company, unless it is your job to manage one of our official Company social media accounts. You should uphold the Company's reputation as The Caring Company – avoid making defamatory statements about members, co-workers, affiliates and competitors.

Use of Artificial Intelligence

Artificial intelligence has become a powerful tool with a wide variety of applications.

Associates can use these tools but must follow these basic rules:

- Approved tool: Microsoft Copilot with Enterprise Data Protection is the approved tool for ad hoc business generative AI use. Any of the models (Claude and GPT as of this printing) provided for your use within Microsoft Copilot are acceptable to use for business purposes. However, public versions of these same tools and any other publicly available or purchasable versions of Generative AI are unacceptable and are prohibited for business purposes.
- Data: Sensitive or proprietary data—such as PHI, PII, member information, confidential documents, source code, pricing, strategy, or non-public information—must not be entered into public AI tools.
- Devices: Business-related AI prompts must use BCBSAL workstations—not personal or mobile devices.
- Accountability: AI output must be reviewed for accuracy, completeness, copyright/proprietary content, and appropriateness before use; users remain accountable for work products created with AI. AI use is logged and monitored by Information Security, and violations may lead to disciplinary action.
- New use cases: New or high-risk AI use cases must go through governance review, risk assessment, and appropriate controls for fairness, privacy, security, accuracy, compliance, and transparency.
- Meetings: AI is not to be used to capture transcripts of meetings or create meeting summaries.

Refer to the Artificial Intelligence Corporate Operating Policy for more detailed information on appropriate use of AI.

Table of Contents

WORK SUCCESSFULLY WITH OUTSIDE ENTITIES

Our Codebook is also provided annually to our First Tier, Downstream, and Related Entities (FDRs) and vendors. While every aspect of the Codebook may not be applicable to our FDRs and vendors, it is important to our Company that we clearly communicate the requirement to conduct our business in an ethical manner, and we expect any business conducted on our behalf will be done in accordance with our values. We also expect FDRs and vendors to report issues regarding the work they do for Blue Cross and Blue Shield of Alabama as well as to participate in any investigation regarding activities that have been performed on our behalf that may have legal or ethical implications.

FDRs and vendors, as well as any workforce member employed with an FDR or vendor, may contact Blue Cross and Blue Shield of Alabama regarding concerns or questions using any of the avenues outlined in the Codebook.

Working with Vendors

In your position with the Company, you or your family members may not receive special favors or rebates from the Company's vendors or suppliers. These may be considered kickbacks and are against the law.

Kickbacks or rebates can take many forms and are not limited to direct cash payments or credits. In general, if you or your family stands to gain personally through a transaction with a vendor, supplier or provider, it is prohibited. Such practices are not only unethical but are illegal in many cases.

A kickback is defined as any money, fees, commission, credit, gift, gratuities, things of value, or compensation of any kind which is provided, directly or indirectly, for the purpose of improperly obtaining or rewarding favorable treatment in connection with a contract.

Some examples include:

- A vendor offers tickets to the Super Bowl in return for business;
- A competitor offers cash or a consulting contract in return for Company trade secrets; or
- A provider offers a gift for preferential treatment (e.g., inclusion in the network, placement at top of list for referrals, expediting claim payment).

The Company is required to prevent and detect kickbacks in its own operations by the federal Anti-Kickback Statute. The Anti-Kickback Statute prohibits anyone from knowingly and willfully offering, paying, soliciting or receiving a kickback, bribe or rebate in connection with an item or service which may be paid under a government contract. This includes kickbacks and rebates to or from a vendor, provider, or government agency or any of their employees in connection with giving or receiving favorable treatment under a federal healthcare program.

The Anti-Kickback Statute imposes severe criminal, civil and monetary penalties not only on individuals who offer the kickbacks, but also on the Company and its associates who solicit or accept such items. We are required to report when there are reasonable grounds to believe a violation of the Anti-Kickback Statute has occurred. Accepting a kickback, as well as not reporting a suspected kickback to the Compliance Office, can result in disciplinary action.

If you have a question whether a benefit could be considered a kickback or rebate, contact the Compliance Office.

Reciprocity

The Company may purchase goods and services from a supplier who also buys goods or services from us as a customer. This practice is normal and acceptable. You may not put any pressure on a supplier or customer, or give the impression that "reciprocity" is expected.

You must not ask suppliers to buy our products or services in order to become or continue to be a supplier of the Company. **There are no exceptions to this rule.**

Subsidiaries, Subcontractors, Consultants, Agents and Vendors

The Compliance Office distributes the Code of Ethics and Business Conduct to third party agents and contractors who act for, or on behalf of, the Company. The Compliance Office shall inform all such parties of the Company's requirement of strict adherence to the Code of Ethics and Business Conduct. The Compliance Office also distributes the Code of Ethics and Business Conduct to vendors who conduct significant business for the Company in order to provide a description of our values and expectations. If you have any concerns about a vendor's business practices or results, notify the Compliance Office or call the Compliance Help Line.

Payments to Agents, Representatives and Consultants

Any agreement with an agent, sales representative or consultant must be in writing and must clearly and accurately set forth the services to be performed, the basis for earning the commission or fee involved, and the applicable rate or fee. Any payments must be reasonable by industry standards and according to the amount and value of the services provided.

You must not ask suppliers to buy our products or services in order to become or continue to be a supplier of the Company.

Business Associates

A "business associate" is a person or entity that

- Performs certain functions or activities that involve the use or disclosure of PHI on behalf of the Company, or
- Provides services to the Company that involve the use or disclosure of PHI.

Any vendor or contractor who may have access to PHI in the course of providing functions or activities to or on behalf of the Company is a business associate. Before any vendor or contractor gains access to PHI, a business associate agreement (also known as a BAA or BAK) between the vendor or contractor and the Company must be in place. Associates involved in contracting with such entities are responsible for making sure a BAA is in place. This is a Company requirement as well as a requirement under HIPAA Rules.

Delegated Entities and First Tier, Downstream, and Related Entities

Delegated Entities are vendors to whom the Company has delegated administrative and healthcare functions performed under our Medicare Part C and Part D contracts and our Qualified Health Plans (QHPs). Delegated entities are further categorized as First Tier, Downstream, and Related Entities (FDRs) under the Medicare Part C and D regulations as well as under regulations governing QHPs. The delegated entity with whom the Company would contract to provide these services is called a First Tier Entity. If the First Tier Entity contracts with another vendor to provide the services to the Company, that entity is called a Downstream Entity. A Related Entity would be a subsidiary of an organization (such as the Company) that provides services under the Medicare or QHP plans.

Before the vendor provides delegated services under Medicare Part C or D or QHP plans, a Delegated Oversight Addendum (also known as DO Addendum) must be in place between the vendor and the Company. Blue Cross associates involved in contracting with such entities are responsible for ensuring that a DO Addendum is in place.

Working with the Government

There are special laws under government programs such as Medicare Part C, Medicare Part D and the Federal Employee Program (FEP) as well as for health plans to which the Health Care Reform regulations apply. It is Company policy to abide by these laws. If you have responsibilities in Medicare, FEP or a specific government program, you must be sensitive to situations that could be considered a reward or an inducement for special treatment or could cause or create the appearance of favoritism.

Government Contracts

If you are involved, directly or indirectly, with the Company's government contracts – such as the FEP, Medicare Advantage (Part C) or Medicare Part D – you should consult your manager or the Compliance Office about special rules that may apply.

Preparation and Submission of Proposals and Budget Requests to the Federal Government

If you are involved in the preparation of a proposal to the government, such as those for Medicare Part C or Part D, or our QHPs offered through the Federally Facilitated Marketplace, you have the responsibility to ensure that all data is current, accurate and complete. All those who prepare documentation, sign or in any way support the Company's certifications and representations of accuracy and truthfulness to the government must be extremely careful and accurate. False information or false certification and attestation can lead to civil and criminal sanctions for the Company as well as for the individual involved.

Reports to Regulatory Entities

You are expected to provide full, fair, accurate, timely and understandable disclosure in the reports required to be filed by the Company with any regulatory entity.

Cooperation with Government Inquiries

From time to time, the Company may be asked to cooperate with a government investigation or to respond to a request for information from the government about how we conduct our business. The request may come through official channels from the government to Company management, or you could be contacted individually by a member of an enforcement agency, such as the Federal Bureau of Investigation, the Office of Inspector General or the Department of Justice.

It is our Company's policy to cooperate fully on all such matters. To ensure that this process is conducted efficiently, immediately notify the Compliance Officer and the Legal Department to inform them when you have been contacted by a government representative. Of course, the decision of whether to cooperate with their inquiry is up to you alone, and you will not be disciplined, punished or otherwise retaliated against if you decide to do so. However, if you decide to speak with government representatives, be sure that you are accurate and truthful in all your answers to their questions. If you are not, both you and the Company could be subject to criminal prosecution.

Although Company associates are free to cooperate individually with government investigators, you may not provide documentation or data that belong to the Company, or are in its custody and control, in response to a government request for information without first obtaining authorization from the Compliance Office and Legal Department.

Employment of Government Personnel

There are special rules about recruiting and hiring current and former federal government employees, including military and civil service employees. These rules also apply to individuals the Company hires and retains as consultants. Violations could result not only in sanctions against the former government employee, but the Company could also be held criminally or civilly liable. Consult Staffing Resources or the Compliance Office with any questions.



Political Activity and Contributions

Federal laws restrict the use of corporate funds in connection with federal elections. You may not use Company funds, property, facilities or Company-work time for any political activity, such as asking for political contributions, mailing campaign materials or making phone calls. Candidates for office will be allowed to present their views and address the management of the Company from time to time under the following circumstances:

- All legitimate candidates are provided an equal opportunity to express their views;
- The presentation is structured as a public service and a forum for discussion of the issues. Invitations are extended and requests granted on a non-partisan basis, regardless of political party affiliation;
- Attendance is optional;
- Fund raising is not allowed; and
- The presentation does not interfere with productivity.

Allowing a forum to discuss a candidate's political platform should not be interpreted as an endorsement by the Company.

Special Responsibilities

If Your Job Requires Licensure/Credentials

If your position requires you to have a certain license or credentials, you are ultimately responsible for maintaining licensure or credentialing. If you lose licensure or credentialing required by your position, you are responsible for notifying your manager or department head immediately. Managers have the responsibility to ensure that their associates maintain licensure or credentialing required for their positions. Please consult your management team on any specific departmental requirements or processes regarding the documentation of proof of licensure in good standing or renewal of licensure.

If you become the subject of an investigation by a regulatory board, professional credentialing, or licensing body, you have a duty to report this investigation to the Compliance Office at ComplianceOffice@bcbsal.org.

If You Are a Manager or Supervisor

All management and supervisory personnel are responsible for ensuring that Blue Cross and Blue Shield of Alabama complies with applicable laws and regulations and the Company's Code of Ethics and Business Conduct. Individuals in management and supervisory capacities will be appropriately disciplined, up to and including termination of employment, for failure to instruct others or for failure to detect noncompliance with applicable policies and legal requirements if reasonable due diligence on the part of the manager or supervisor should have led to the discovery of any problems or violations.

Corporate Compliance Officer and Medicare Compliance Officer

The Corporate Compliance Officer and the Compliance Officer for Medicare Parts C and D are responsible for oversight of compliance with applicable laws, the Code of Ethics and Business Conduct, and related policies and procedures. The Compliance Officers report to the Board of Directors, President and Audit Committee on the implementation and enforcement of the Compliance Program and provide periodic

updates to the appropriate committees of the Board of Directors. The Compliance Officers request the assistance of General Counsel and Internal Audit when appropriate. Any waivers of violations awarded by the Compliance Officer will be reported to the Audit Committee of the Board of Directors.

Company Attorneys

Company attorneys have the additional obligation to report evidence of a material violation of law or breach of fiduciary duty or similar violation by the Company or any controlled affiliate, or any of their agents, to the General Counsel or the Chief Executive Officer of the Company. If the General Counsel or Chief Executive Officer does not appropriately respond to the evidence, the Company attorney shall report the matter to the Audit Committee of the Board of Directors of the Company or to another committee of the Board of Directors comprised solely of directors not employed directly or indirectly by the Company or the Board of Directors.

Powers and Fiduciary Duties of Directors and Officers

The Company operates through its associates, managers, officers and directors. The Board of Directors (BOD) makes fundamental management and policy decisions by adopting provisions in the Company bylaws or through resolutions made at BOD meetings, such as the adoption of this Codebook.

The Board of Directors has five primary functions:

1. **Select** senior management and determine their compensation;
2. **Review and approve** Company policies, financial objectives, major strategies and plans;
3. **Provide advice** and counsel to top management;
4. **Select** candidates for the BOD and evaluate Board processes and performance; and
5. **Institute** policies and procedures to further the goals of the Company.

In order to carry out its primary functions, the BOD is charged with obligations and duties in overseeing the business conduct and ethical standards of the Company. The BOD has a fiduciary duty to protect the assets of the Company and ensure their efficient use. All Company assets should be used for legitimate business purposes. Both the BOD and officers have a fiduciary responsibility to the Company. This means the BOD and officers are required to exercise their powers in good faith solely in the best interests of the Company. When an individual accepts the position of director or officer, that person agrees to give careful attention to the Company's concerns and to be faithful and honest in the performance of their duties.

The BOD does not carry out the day-to-day management of the Company; that function is left to the officers, managers and other associates. The officers of the Company also have a fiduciary responsibility to act in the Company's best interest. The Company bylaws further outline the duties, activities and obligations of the officers. If the financial statements of the Company, or an affiliated company, must be restated due to misconduct, the officers will reimburse the Company for any bonuses received during the 12-month period following the issuance or filing of the financial statements.

In performing their management role, the officers must act in a manner consistent with the standards of the Company, and execute specific plans, policies and directives from the BOD. The officers, together with the BOD must ensure that every director, officer, manager and associate complies with this Code of Ethics and Business Conduct.

APPENDIX A

Sample letter for return of cash, check, gift certificate or gift card

Date

Name of Company
Street Address
City, State, Zip Code

Dear _____,

I received your (cash, checks, gift certificates, gift card) for (reason for the gift) and your thoughtfulness is appreciated.

Blue Cross and Blue Shield of Alabama associates are not allowed to receive gifts of cash, checks, gift certificates or gift cards of any kind. We have adopted this practice as a part of our Code of Ethics and Business Conduct to ensure we use the highest ethical standards in doing business with our customers, vendors and providers.

Being reinforced for a job well done is always appreciated. If you would like to express appreciation, it would be a kind and generous act if you would consider a small donation to your favorite charity. I am returning your (cash, check, gift certificates, gift card). Again, thank you for your thoughtfulness.

Sincerely,

Associate's Name
Title

Enclosures
cc: Compliance Office

Sample letter for accepting or declining a conference or event

Date

Name of Vendor, Group, or Provider
Street Address
City, State, Zip Code

Dear _____,

Thank you for your invitation to participate (in the event, conference, etc.) (Month, Day) through (Month, Day, Year), in (City, State). Your offer to pay my hotel, airline flight and (entrance fee, registration fee, etc.) is appreciated.

Blue Cross and Blue Shield of Alabama associates are not allowed to accept travel expenses or honoraria. We have adopted this practice as a part of our Code of Ethics and Business Conduct to ensure that we use the highest ethical standards in doing business with our customers, vendors and providers.

We strive not to do or accept anything that would appear to be improper to the public, our customers or our regulators. When the opportunity to attend events such as yours is offered, the expenses of attending are Blue Cross and Blue Shield of Alabama's responsibility.

(Option #1)

However, I do wish to attend (the event, conference, etc.). Please provide me with the registration information. I will contact the hotel and airline to make reservations.

Your thoughtfulness in offering to have me as your guest is appreciated, but because of our corporate policy, I must decline your generous offer.

I look forward to seeing you (Month Day, Year).

(Option #2)

Unfortunately, I will not be able to attend because of a prior commitment; however, I know that (the event) will be very successful. Your thoughtfulness in offering to have me as your guest is very much appreciated.

Sincerely,

Associate's Name
Title

cc: Compliance Office

APPENDIX C

Laws and Regulations

One of the purposes of our Compliance program is to educate associates about our obligations under the law. Our Company is subject to a variety of laws and regulations with which we must be familiar and comply. These laws and regulations include:

HIPAA Regulations

Health Insurance Portability and Accountability Act (HIPAA)
HIPAA addresses many different parts of health insurance. The privacy portion of the law ensures that an individual's identifiable health information is not used or disclosed except under certain circumstances or if the individual authorizes its release. The security portion of the law deals specifically with Electronic Protected Health Information (ePHI). It outlines three types of security safeguards required for compliance: administrative, physical and technical. Both civil and criminal penalties are possible when a violation of HIPAA occurs.

Employment, Human Resources and Workplace Environment Laws

Americans with Disabilities Act (ADA)
The ADA prohibits discrimination on the basis of disability in employment, state and local government, public accommodations, commercial facilities, transportation and telecommunications.

Civil Rights Act of 1964 (Title VII)
Title VII of the Civil Rights Act prohibits discrimination by covered employers on the basis of race, color, religion, sex or national origin. Title VII also prohibits discrimination against an individual because of his or her association with another individual of a particular race, color, religion, sex or national origin.

Drug-Free Workplace Act of 1988
The Drug-Free Workplace Act of 1988 requires all organizations receiving federal grants to maintain a drug-free workplace. The act requires that all associates be trained annually on the Drug-Free Workplace Act.

Employee Retirement Income Security Act of 1974 (ERISA)
The Employee Retirement Income Security Act of 1974 is a federal law that sets standards for most voluntarily established pension and health plans in private industry to provide protection for individuals in these plans.

Violent Crime Control and Law Enforcement Act
This law prohibits individuals who have been convicted of specified criminal activity from engaging in the business of insurance without written consent from the Commissioner of Insurance.

Family Medical Leave Act
The act entitles employees to take reasonable leave for medical reasons, for the birth or adoption of a child, and for the care of a child, spouse or parent who has a serious health condition.

Federal Contract Administration Laws

Anti-Kickback Act
The Anti-Kickback Act is a criminal statute that prohibits anyone from knowingly or willfully paying or receiving compensation in exchange for referrals or the purchase of any item or service that may be paid by a federal healthcare program.

False Claims Act
The False Claims Act is a civil statute that prohibits the knowing submission of false or fraudulent claims to the government for payment.

Medicare Advantage (Part C)
Medicare Advantage, also known as Medicare Part C, is an option Medicare beneficiaries can choose to receive most or all of their Medicare benefits through a private insurance company.

Medicare Prescription Drug Program (Part D)
Medicare Part D is prescription drug coverage available on its own or as part of a Medicare Advantage plan (Part C) with prescription drug coverage.

Federal Employees Health Benefits Program
The Federal Employees Health Benefits Program (FEHBP) provides health insurance to employees of the U.S. government through a variety of options.

Patient Protection and Affordable Care Act
The Patient Protection and Affordable Care Act (PPACA), along with The Health Care and Education Reconciliation Act, are the two federal statutes signed into law in 2010 to cover a number of changes in health insurance, also known as Healthcare Reform.

Mail and Wire Fraud Statutes
Mail fraud refers to any scheme which attempts to unlawfully obtain money or valuables in which the postal system is used, at any point, in the commission of a criminal offense. Wire fraud is when an individual devises any scheme to defraud, or obtain money or property by making a false or fraudulent statement or promise. As a result of this misrepresentation, the money or property is transmitted by wire, radio or television communication across state lines.

Insurance Fraud Statutes
Insurance fraud is when an individual intends to defraud or deceive any insurer, by presenting false information in connection with an application for any policy of insurance or claim for payment or other benefit from a plan providing healthcare benefits.

Computer Fraud and Abuse Act
The act makes it unlawful for any person to access a protected computer without authorization and forbids a person who has a legitimate and authorized right of access from exceeding the authorized access.

False Statements Act
The False Statements Act prohibits a person from making a false or misleading statement or withholding material information in connection with the delivery of services to or payment from the government.

Telephone Consumer Protection Act (TCPA)
The Telephone Consumer Protection Act (TCPA) regulates certain telemarketing calls, prerecorded calls, autodialed calls and unsolicited faxes.

The No Surprises Act
The No Surprises Act prohibits surprise bills for consumers for out-of-network emergency services, out-of-network air ambulance services, and certain out-of-network services received at in-network facilities.

The Transparency in Coverage Rule
The Transparency in Coverage Rule requires health plans to create a member-facing price comparison tool and post publicly available machine-readable files that include in-network negotiated payment rates.



BlueCross BlueShield of Alabama

An Independent Licensee of the
Blue Cross and Blue Shield Association

Table of Contents