CODE BLUE

Blue Cross® Blue Shield® of Arizona's

CODE OF CONDUCT 2024-2025

A GUIDE FOR EMPLOYEES, OFFICERS, AND BOARD MEMBERS OF
BLUE CROSS BLUE SHIELD OF ARIZONA, AND ITS WHOLLY OWNED SUBSIDIARIES AND AFFILIATES

WE INSPIRE HEALTH AND MAKE IT EASY!

Table of Contents

Dear Employees, Officers, and Board Members,

For 85 years, Blue Cross Blue Shield of Arizona (AZ Blue) and its subsidiaries and affiliates—"the Company"—have enjoyed the privilege of helping Arizonans care for their health and well-being. Over time, they have come to trust us to do the right thing; to believe we have their best interests at heart.

We absolutely do.

In fact, we continue to exist because we keep earning that trust. We operate responsibly and ethically, adhering to the code of conduct we call Code Blue.

Code Blue is the pledge we take to protect our members' privacy, to conduct ourselves with integrity, and to adhere to federal and state laws and regulations. Each year, we renew this pledge and participate in required training to ensure these obligations remain ingrained in our actions.

Within the Code Blue document, you will find guidance to help you do your part in upholding this pledge, including:

- The company mission and values
- An outline of specific legal requirements
- Information on Company policies
- Examples of acceptable and unacceptable behavior
- Where to direct your questions and report concerns

As a Company employee, officer, or board member, you are responsible for studying and knowing Code Blue, for completing the annual mandatory training, and for ensuring that we all meet the expectations described in this document.

If you see behavior that is unethical or potentially harmful to someone or to the Company, we ask that you report it. Depending on how you're most comfortable communicating the issue, you can:

- Contact Chief Compliance and Privacy Officer Anne Schrock (ext. 4315) or the Corporate Integrity department (compliance@azblue.com) with your questions or concerns;
- Share your concerns with your manager;
- Talk to the compliance officer for your Organization as listed in the Appendix; or
- Call the Compliance Hotline at 1-888-474-3683.

While the Company's No-Retaliation policy protects employees who report unethical behaviors, you may also choose to remain anonymous when you call the hotline. You choose the reporting method you feel most comfortable using.

Code Blue is integral to our daily work and to our enduring reputation as a trustworthy organization. Thank you for helping AZ Blue maintain the highest ethical standards for the Company, its customers, and the people of Arizona.

Pam Kehaly
President and CEO
Blue Cross Blue Shield of Arizona

Inspiring Health with Compliance

It is our mission to Inspire Health and Make It Easy as Arizona's trusted leader in delivering affordable, innovative, and accessible healthcare solutions. In order to achieve this mission, we collaboratively engage in building honest relationships with our customers, suppliers, vendors, and providers.

By collectively engaging in building relationships, we uphold our values. We are dedicated to doing our part in making the state of Arizona a healthier place for all. We are **caring** by always putting customers first and we are **accountable,** fulfilling all of our commitments. We strive to be **curious** and embrace the opportunity to learn and innovate while being **inclusive** and embracing our differences. And we are **collaborative** by listening to and communicating with each other to achieve shared goals.

We conduct our business activities in a transparent, open, and truthful manner. We do not sacrifice our compliance and ethics concerns in order to accomplish personal or corporate goals.

By making compliance and ethics a part of our routine responsibilities (on and off the job), we can Inspire Health and Make It Easy by providing the best value in health insurance and related health services efficiently to improve the quality of life for Arizonans.

MISSION

It is our mission to inspire health and make it easy

VALUES

Caring
I put people and community first

Curious
I learn, change, and innovate

Accountable
I take responsibility and meet my commitments

Inclusive
I embrace differences

Collaborative
I listen and communicate to achieve shared goals

Ask QUESTIONS | **Report** CONCERNS

Introduction

As a part of our commitment to compliance, AZ Blue has developed and implemented standards applicable to all employees, officers, and board members that detail the manner in which we conduct business on behalf of AZ Blue, its affiliates, and its wholly owned subsidiaries ("the Company").

These standards are described in the various sections of Code Blue, the Company's code of conduct. Code Blue is based on a strong commitment to compliance and ethical practices by the Company's boards of directors and senior management and offers a clear and concise collection of company-wide principles and standards. Code Blue is the cornerstone of the Compliance & Ethics Programs of each individual entity of the Company (Organization) (i.e., Medisun, Health Choice Arizona, and Prosano Health).

Code Blue details the fundamental principles, values, and framework for conducting business properly and professionally that we employ in our interactions with customers, members, patients, vendors, government regulators, local communities, and the environment. Code Blue affirms our Company's commitment to complying with all federal and state laws and regulations. Code Blue is reviewed annually and updated as needed. Code Blue and your Organization's Compliance & Ethics Program are available on your Organization's intranet site. Code Blue is also available on AZ Blue's public website, **azblue.com.**

Code Blue is a set of principles based on the laws, regulations, and corporate policies that affect us. These policies apply to all employees, officers, and board members of the Company. They describe the behavior required for initial and continued employment.

We are expected to perform our jobs consistent with Code Blue. Nothing in Code Blue precludes lawful action by employees. The Company looks at how we apply the principles of Code Blue in our everyday activities as part of our annual performance evaluations and promotion decisions.

To have a corporate-wide culture of ethical behavior, we must understand what to do when we face an ethical or compliance concern. Code Blue provides the foundation for making ethical decisions and includes the many ways we can report known and suspected inappropriate behavior, actions, fraud, waste, and abuse.

Ways to report:

- Speak to your supervisor, manager, director, or vice president.
- Ask to meet with your Organization's compliance officer, the privacy officer, or a member of the Compliance Committee or the Compliance, SIU, Legal, or Human Resources departments, listed in the Appendix.
- Call the Compliance Hotline at **1-888-474-3683.** (You can remain anonymous.)
- Email compliance@azblue.com.
- Review the Appendix for other ways to report concerns, including hotline and email info.

Code Blue covers:

- Legal Compliance
- Accurate Data
- Record Retention
- Protection of Non-Public Information
- Conflicts of Interest
- Relationships with Vendors, Contractors, Customers
- Government Contracts
- Anticompetitive or Unfair Trade Practices
- Government Investigations
- Fraud, Waste, and Abuse Prevention, Detection, and Correction
- Corporate Assets
- Political Activity
- Workplace Issues
- Reporting Requirements and Our No Retaliation Policy

Our Role:

- Know the laws and regulations that apply to our jobs.
- Ask questions when in doubt.
- Treat others with honesty and respect.
- Take responsibility for our actions.
- Report known or suspected inappropriate behavior, actions, fraud, waste, and abuse.

Reporting Violations of the Code

As team members, we all have a responsibility to report potential or actual violations of Code Blue. We have many ways to report suspected violations of Code Blue without fear of punishment or retaliation from the Company or its management. We can discuss matters with our management or use another method to report, such as the Compliance Hotline. The hotline is staffed by an external vendor, 24 hours a day, seven days a week. When making a report, we need to give specific details, whenever possible, so that a proper investigation can be conducted.

Company's Responsibility to Respond

The Compliance Office will investigate all reported Code Blue violations. The compliance officer will report the results to the board of directors. The Company may limit the feedback it provides after an investigation.

The compliance officer, an officer of the Company, or the chief executive officer (CEO) will report actual violations of federal or state law to the appropriate authorities. Our Company and our board of directors will cooperate fully with all government investigations.

No Retaliation Policy

If you make a report in good faith of a suspected violation of Code Blue or of state or federal laws or regulations, including the Affordable Care Act, you will be protected from retaliation. Know that you will not lose your job or be disciplined just because you make a report or ask a question. The Company will do its best to protect the confidentiality and anonymity of anyone who makes a report. However, under certain circumstances, the Company may have to supply the name of the person making the report.

Did you know?

We are **accountable** when we report potential or actual violations of Code Blue as soon as we become aware of them.

Reporting misconduct immediately protects our ethical culture, our reputation, and our ability to do business.

The Company protects us from any form of retaliation if we make a good-faith report of a suspected violation.

Questions About Code Blue?

See the Resources and Contact Info in the Appendix.

Reporting to the Government

The U. S. False Claims Act contains reporting provisions protecting individuals who report concerns to the government. Ways to report to the government include:

- A member of Congress or congressional staff
- The Office of Personnel Management (OPM) Office of the Inspector General
- The Centers for Medicare & Medicaid Services (CMS)
- The Government Accountability Office
- The Arizona Health Care Cost Containment System (AHCCCS)
- A federal employee responsible for contract oversight or management at the OPM
- An authorized official of the Department of Justice or other law enforcement agency
- A court or grand jury

Employees should report:

- Known or suspected instances of gross mismanagement of a federal contract or grant;
- Gross waste of federal funds;
- An abuse of authority relating to a federal contract;
- A substantial and specific danger to public health or safety;
- A violation of a law, rule, or regulation related to a federal contractor.

Issues can be reported to our Organization's compliance officer or compliance department, or the Compliance Hotline. Employees who report misconduct to the government are protected from retaliation. While the False Claims Act was enacted as a way for people to report wrongdoing to the government, each organization has a Compliance & Ethics Program in place so employees can report potential wrongdoing internally.

SECTION 1

Ethical Professionalism Requires Legal Compliance

We obey the law at all times when conducting Company business.

Code Blue is part of the Company's Compliance & Ethics Program. The program was created to help us understand our duty under and beyond the law.

There are many laws and regulations that affect the way we do business. Some of these laws control:

- Arizona Department of Insurance and Financial Institutions licensing
- Accuracy in record keeping
- Privacy
- Physician self-referrals or remuneration for referrals
- Unfair trade practices
- Participation in federal medical programs such as the Marketplace for Qualified Health Plans, the Federal Employee Program® (FEP®), and Medicare
- Arizona Health Care Cost Containment System (AHCCCS) Medicaid rules

We must all know about the laws and regulations that apply to our jobs.

We must follow established Company policies and procedures. We can locate the policies for our Organization in the Appendix. The Company provides training on general policies and compliance issues through live and online training, and as part of departmental meetings. Specific programs are also offered for each of our individual lines of business, as needed.

Beyond legal requirements, policies, and procedures, we live our values. The values are listed on page 4.

Code Requirements

We are each responsible for:

- Following the laws and regulations that apply to the Company.
- Following our Organization's policies and procedures.
- Adhering to our Company values.
- Asking questions when we are uncertain about something.
- Reporting known and suspected violations of laws, regulations or Company policies, and procedures.

SECTION 2

Report Data Truthfully and Accurately

Record and report all financial data and transactions accurately and honestly. Follow proper accounting rules at all times.

We each have a responsibility to ensure that we record truthful and accurate information in everything we do and especially in these critical areas:

- Timecards
- Business expenses
- Production or performance data
- Any other business-related activities we record and/or report on

We must report and record information in connection with Company contracts accurately and truthfully. Do not:

- Distribute or assign costs to contracts that violate the contract's provisions or fail to follow applicable accounting rules
- Inaccurately report labor cost records, or submit or instruct another employee to submit false time charges or assign costs to the wrong contract
- Alter or falsify any information in any record or document that misrepresents the facts
- Try to influence, pressure, or manipulate an auditor to make financial statements that are misleading

Risks of Inaccurate Data

Inaccurate data can lead to fines for our Company, restrictions on our ability to do business, and, in the most egregious circumstances, prosecution.

Did you know?

Even if you are asked to do so by a supervisor or co-worker:

- Do not report data that is not accurate or truthful
- Do not alter or falsify data in any Company record or document

Use one of the options listed under "Reporting Requirements" to ask questions or report incidents. (see page 35)

Ask QUESTIONS | Report CONCERNS

SECTION 3

Follow Records Retention Policies

Keep or destroy all business records based on the law and our records retention policies. This includes all types of stored information:

- Paper records
- Digital records
- Computer files
- Email
- Information stored any other way (on CDs, tape, discs, etc.)

Do not tamper with, remove, or destroy business records contrary to Company records retention policies.

A government investigation, lawsuit, or court order may impose additional records retention requirements, often called *Legal Holds.* When this occurs, carefully follow the instructions from the Company Legal department. Inappropriate destruction of records could constitute a crime.

Know Where to Find Records Retention Information

For more information on records retention, see your Organization's records management policy on your Organization's intranet site. See the Appendix for additional details.

Did you know?

We are **accountable** when we report potential or actual violations of Code Blue as soon as we become aware of them.

The Company protects us from any form of retaliation if we make a good-faith report of a suspected violation.

SECTION 4

Protect Non-Public Information

We have a responsibility to protect non-public information at all times. Non-public information includes Protected Health Information (PHI), Company proprietary information, and other non-public information.

Do not use or give out non-public information to anyone without approval.

Protected Health Information (PHI)

PHI is **individually identifiable health information** and includes:

- Medical records
- Patient information
- Other personal information:
  - Social Security numbers
  - Addresses
  - Phone numbers
  - Financial information (e.g., bank checking account routing information)
  - Email addresses

Access and use of PHI is limited to when it is necessary to complete our job functions. Accessing PHI when it is not needed to complete our job tasks or accessing PHI out of curiosity is strictly prohibited.

If PHI is released accidentally or inappropriately, please notify your supervisor and your Organization's privacy officer right away; additional Privacy contact information can be found in the Appendix. The Company is often required to report inappropriate release of or access to PHI within very short timeframes.

Company Proprietary Information

Company proprietary information is information that relates to the Company's business that the Company wants to keep private and includes:

- The Company's business plans and operations
- Pricing and financial data
- Marketing plans
- Computer software
- Inventions
- Planned business transactions
- Underwriting information
- Information from a third-party vendor that we agreed to keep confidential
- Vendor or hospital contract details and pricing
- Data and lists that show employees and brokers
- Information we do not want competitors to know
- Information marked "Confidential" or "Proprietary"

Other Non-Public Information

Some information we have about others is also non-public information that must be safeguarded. Examples include personal information we have about board members, brokers, employees, providers, and vendors. This includes Social Security numbers, birth dates, addresses, and tax IDs and other information we know because of our employment.

Data Security and Software License Obligations

To ensure maximum protection of our company data, the Company strictly enforces data security provisions. For example, we must protect the integrity of company data by allowing only authorized users to access appropriate information. We refer to access restrictions as the minimum necessary. We must all take every precaution to ensure that user IDs and passwords are not available to unauthorized users.

Sometimes contractors from other companies are brought on site or given access so they can perform work for us. It is important for business owners of these projects to follow the contract requirements and then discontinue access and ensure that Company work papers and equipment are returned when the contract ends.

The Company uses a wide variety of computer software that is protected by various licensing agreements and copyright laws. As employees, we cannot duplicate or use computer software outside the bounds set by the vendor. The penalties for violating these licensing agreements are severe and may include personal liability.

Social Engineering

Be aware of social engineering and phishing scams in which people try to obtain access to non-public information by pretending–in person, on the phone, or through email–to be legitimate. They may pretend to be from Information Technology and ask for your password or try to enter a building under false pretenses. If you suspect phishing, check the Safe Email List on your Organization's intranet, and use the Phish Alert Report option in Outlook. This issue is so important to the viability of the Company that persistent failures will result in performance warnings and potentially termination.

Unsure if the information is non-public information?

Contact your management or the Legal department before releasing the information.

Did you know?

Corporate information technology and Privacy policies are also available on your Organization's intranet. If you have a question related to information security, please call your Organization's service desk as listed in the Appendix.

Protecting Member Privacy

There are multiple policies dealing with privacy. They are located on the AZ Blue intranet. The AZ Blue Identity Verification and PHI Disclosure Grid is a great tool to determine the information we can disclose and to whom.

Privacy Audits

The Privacy Office and Information Security Services (ISS) perform after-hours walkthroughs to monitor compliance with Company privacy and information technology policies.

Helpful Hints:

When sending PHI outside of the company by email, type [SECURE] in the subject line to encrypt the information. This also encrypts any attachments.

Place PHI only in the body of the email or as an attachment, since the subject line is not encrypted.

When sending faxes, use a cover sheet that does not contain PHI. Double-check the fax number before hitting the Send button.

To prevent unauthorized access, protect system passwords the same way we do our Social Security numbers.

Questions about privacy?

Contact your Organization's Privacy Office as listed in the Appendix.

Disclose information only if a valid need exists and you have received proper approval, such as a Confidential Information Release Form (CIRF) or a contract and Business Associate Agreement (BAA) with a vendor. In addition, use, disclose, or request the minimum necessary PHI required to perform the given task. Review all policies and procedures related to disclosure prior to giving out the information.

It is imperative that we are careful to prevent disclosures of non- public information to unauthorized people outside of the Company.

Ways we can help prevent unauthorized disclosures of non-public information:

- Ensure that all non-public information is properly stored.
- Do not discuss non-public information with co-workers in public areas, such as elevators, restrooms, restaurants, etc.
- Remember that our duty not to disclose continues after termination of employment.
- Consult Company privacy and security policies for further information.

SECTION 5

Avoid Conflicts of Interest

Act in the best interest of the Company. We must not take part in activities that conflict with our responsibilities as employees, officers, and board members. We should not compete with or benefit personally from opportunities we discover while using company property.

A conflict of interest is a situation that occurs when our personal interests or activities could influence our decisions. It could prevent us from acting in the best interests of the Company. A conflict of interest includes activities that may only appear to influence our judgment or decisions. Even the appearance of a potential conflict of interest can cause our vendors and customers to question our motives. Our personal interests should not create such a situation.

For this reason, even if it would otherwise be a part of our regular job duties, we are prohibited from processing claims, testing systems, or working on cases that involve information about people we know, such as family or friends. In such instances, always notify your supervisor and hand off the work to someone else.

Conflicts can occur when someone with whom we have a personal relationship or date works for or applies to work for the Company. For instance, if your sibling or in-law applied for work at the Company, they may not be eligible for hire. It may also be against policy to date some Company employees and contractors.

Another example would be if a mother and son both work here and one wants to change jobs within the Company; they may not be allowed to move to a different job. This can occur, for example:

- If, together, both people have the ability to complete an entire transaction
- If one wants to move to a department where sensitive issues may arise (see the accompanying sidebar)
- If one would be reporting to the other
- If one is in a position to review or approve the other's work

Other interpersonal relationships may not improperly influence our business decisions but may have the potential to result in inappropriate workplace conduct. These situations will be referred to the Human Resources department for appropriate action.

It is not unusual or necessarily wrong to have a conflict of interest. Sometimes just the act of disclosing and formally recording the potential conflict is sufficient to resolve it. For this reason, we must keep our Conflict of Interest Form current, updating it as our circumstances change. Do not wait until the annual disclosure period. To access the form, see the Code Blue Appendix.

Did you know?

Employees who work in departments that handle sensitive issues are not allowed to date or have a personal relationship with someone who also works for the Company as an employee or contractor.

The departments include:

- Human Resources
- Internal Audit
- Legal
- Compliance
- Information Security Services
- Special Investigations
- Payroll

The Corporate Integrity department will review and approve all employee moves and new-hire situations involving personal relationships.

A conflict of interest also exists if you or someone with whom you have a personal relationship receives a financial or other personal benefit because of your actions at the Company.

For this reason, the Company will not purchase goods or services from:

- Officers or employees
- A business in which the Company is aware that an employee, or someone with whom an employee has a personal relationship, has a substantial interest

In addition, to avoid these conflicts, board members, officers, and employees must disclose any financial interests they have in competitors or in companies doing business (or seeking to do business) with the Company. If any person with whom an employee has a personal relationship has financial interests in competitors or in companies doing business (or seeking to do business) with the Company, that information would also have to be disclosed.

Laws prohibit loans or extensions of credit of any kind to officers and board members.

Examples:

- If your spouse has a financial interest (5% or more ownership) in a company seeking to do business with the Company, your loyalty to the Company could conflict with your personal financial interests.
- The same conflict could exist if you or your parent have a financial interest in a Company vendor.
- If a company seeking to do business with your Organization offers you a gift or loan, the acceptance of a gift or loan from a potential business partner could compromise your ability to act in the best interests of the Company, and would have to be refused.

See Section 6 for rules on the acceptance of routine business courtesies.

We must also make sure that any second jobs we take do not create any conflicts of interests and that Company time and assets, such as computers and proprietary information, are not used to pursue a second job.

Second jobs we cannot accept

We cannot accept jobs as a consultant, director, officer, or part-time employee of any of the following:

- Competitors
- Subcontractors
- Providers
- Vendors
- Others seeking to do business with Company

As an example, an employee cannot work part-time for a hospital, physician, or care facility. However, the compliance officer may approve exceptions if allowed under state or federal law.

Board members of AZ Blue should also refer to the Corporate Governance Guidelines.

Did you know?

A Personal Relationship includes any individual living in your home or your spouse, parent, child, sibling, grandparent, grandchild, in-laws (mother, father, brother, sister, daughter, son), stepchild, stepparent, or domestic partner.

We are not permitted to date someone within our reporting relationship (where one employee has direct or indirect oversight of an employee they are dating).

To avoid potential conflicts of interest, we are not permitted to, or to ask others to, process claims, test systems, or work on cases that involve people we know, such as family or friends. You should notify your supervisor and hand off the work to someone else.

How Does the Conflict of Interest Disclosure Form Process Work?

- At least once per year the Compliance department will distribute a Conflict of Interest Disclosure Form to all board members, officers, and employees.
- You must also update your Conflict of Interest Form anytime your circumstances change. To access the form, see the Code Blue Appendix.
- You must answer all questions fully and accurately, even if you have given this information before.
- The Compliance department reviews the answers to the Conflict of Interest Disclosure Form and prepares a report of any potential conflicts identified.
- The Compliance department, with advice from the Legal department, then determines what recommendations to make to management and/or the board to eliminate or avoid any identified conflicts of interest.
- The Compliance department documents decisions and recommendations regarding any actual or potential conflicts.

Ask QUESTIONS | Report CONCERNS

Did you know?

You must report any second jobs to your supervisor, regardless of whether they may pose a potential conflict.

Q&A

Q: "Do we report any job changes by a family member or other personal relationship that could be a conflict right away, or do we wait for the annual form process?"

A: Report the change right away to the Compliance department by filling out a new form.

The Conflict of Interest Disclosure Form is available via SharePoint with a link in the Appendix.

Example

Q: "My brother lives in Texas and works for a hospital there. He does not live with me. Do I have to disclose this information on my Conflict of Interest Disclosure Form?"

A: Yes. A brother is considered to be a personal relationship under the Code, regardless of where he lives. You should describe what he does at the hospital.

SECTION 6

Dealing with Suppliers, Contractors, and Customers

Conducting business with suppliers, customers, and contractors can pose ethical or even legal problems. The following guidelines can help us make the right decisions in potentially inappropriate situations.

Kickbacks and Rebates

Do not accept any kickbacks or rebates connected to a purchase or sale of goods and services, or patient referrals. This restriction also applies to your Personal Relationships as described in Section 5. Kickbacks or rebates can take many forms and are not limited to direct cash payments or credits. In general, if you or someone with whom you have a personal relationship could gain personally through the transaction, it is prohibited.

For example, a kickback could be disguised as:

- An offer for a large discount on a new air conditioner for your home or your parent's home, in exchange for contracting with an air conditioning company for the Company
- Use of ABC company's condo in San Diego for a weeklong vacation after you renew ABC's group plan
- A free night's stay at a hotel for you, after you book a convention on behalf of the Company
- Payment from a Durable Medical Equipment (DME) provider for referring patients

Reciprocity

Often the Company purchases goods or services from a supplier who also buys services from us. This practice is normal and acceptable, but any form of pressure for "reciprocity" from either party is not. Suppliers must not be asked to buy our products or services in order to become or continue to be a Company supplier. Likewise, the sale of our products and services will not be dependent upon an agreement that we purchase goods and services from the potential member or account.

Charitable Contributions

The Company follows applicable anti-kickback rules when making charitable contributions. Anti-kickback rules prohibit money or gifts from going into personal accounts of plan group benefit administrators in exchange for consideration for becoming or remaining a customer. We as a company and you as an individual are not allowed to make or imply that charitable contributions will be made in exchange for an individual or a group becoming or remaining a Company customer.

Appropriate Coverage

At the Company, we gain our members' trust and business because of the quality and value we offer. We **Inspire Health** when we thoughtfully make decisions about our members' coverage and base those decisions on appropriateness of the care and the terms of their health insurance policy. The Company does not compensate for denial of coverage or services or offer incentives to providers, officers, or employees that are against any laws or regulations or with the intent to reduce or deny appropriate care or service.

Q&A

Q: "The Company is very interested in purchasing a computer vendor's software. I was invited to a first-class, all-expenses-paid trip to San Diego for a training class to learn more about the product. Can I accept this all-expenses-paid trip to San Diego?"

A: Each situation is different, so consult with your management or the compliance officer. In this scenario, it appears that attending this training class would be in the best interest of the Company. It would be appropriate to attend, but only if the Company pays for the travel expenses, based on our corporate policies. We cannot allow vendors to pay for travel expenses without prior approval by the CEO or CFO.

See your Organization's policies for further guidance on travel.

Business Courtesies

A business courtesy is a gift or favor for which we pay nothing or less than fair market value. It may include such items as:

- Gifts
- Transportation
- Discounts
- Tickets
- Passes
- Promotional items
- Use of a giver's time, materials, or equipment

If you or your management is uncertain about accepting or giving a business courtesy, you should decline to do so. The compliance officer and the Corporate Integrity department are available to assist you, should you need additional guidance.

What May We Accept?

Yes: Infrequent, inexpensive promotional items, such as company mugs or T-shirts, valued at less than $100, and prize items won at raffles from vendors at conferences.

No: Cash, checks, gift cards issued by a bank or financial institution (e.g., VISA®/ Mastercard®), expensive gifts, computers, cell phones, lottery tickets, etc. Gift certificates and gift cards to restaurants or retail stores may be accepted, as long as they are not to expansive retailers such as Amazon, Costco, and Sam's Club and as long as they are not from a member. All gift certificates and gift cards should be reported to the Corporate Integrity department.

No: Repetitive gifts from the same vendor, provider, or customer for which the cumulative value exceeds $100 (for example, event tickets worth $75 each that are received more than once in a year). You are expected to decline or return such items when the cumulative value reaches $100. You cannot accept the gift and then give it to someone else.

Others, or if you have questions: Ask your management or contact your Organization's compliance officer or the Corporate Integrity department.

Government programs have special rules on gifts. See Section 7 for more information.

Acceptance of Business Courtesies

We can never accept gifts of money or solicit gifts or favors for personal use from suppliers, customers, contractors, or providers. We or someone with whom we have a Personal Relationship are permitted to accept business courtesies from a business or individual doing or seeking to do business with the Company only if the courtesy is:

- Unsolicited
- Non-monetary
- Infrequent
- Inexpensive (generally no more than $100 retail value – individual situations may vary and should be discussed with the compliance officer)
- Approved in advance, when possible, by management

There are times when we may be able to accept expensive business courtesies of more than $100 retail value if protocol, courtesy, or other special circumstances exist. These should be reported right away to your management, the compliance officer, and in writing by filling out a new Conflict of Interest Disclosure Form. The compliance officer will determine if we may personally accept, refuse, or return a gift, or whether it should become Company property.

Holiday Gifts

Gift giving increases during the winter holidays. Members, vendors, and others express their appreciation for exemplary service and good working relationships. Guidance material on acceptable gifts and ways to handle unacceptable gifts is in the Compliance policies located on your Organization's intranet. You can view locations of your Organization's policies in the Appendix. If you are not sure about a gift, contact your Organization's compliance officer.

Gifts from Patients

Some patients may offer clinicians gifts as an expression of gratitude. Some gifts may be intended to influence care or preferential treatment. Physicians should report gifts to their Organization's compliance officer, and should consider the following before accepting or declining a gift:

- Is the gift extravagant?
- Would acceptance of the gift influence the physician's delivery of care, or influence the patient's expectations regarding their care?
- Would accepting the gift create an emotional, financial, or other hardship for the patient?

Clinicians may wish to suggest to the patient that the patient make a donation to a charity in lieu of a gift.

Did you know?

What May We Accept?

Yes: Once each year, a key vendor invites us to their hospitality suite for a Phoenix Suns game. The vendor is attending and has invited at least 20 other people from different companies. The cost is unknown.

Depends: Once each year, a key vendor offers general admission tickets or admission to a skybox at the Phoenix Open golf tournament or the Super Bowl when held in Arizona. It is best to contact your Organization's compliance officer for specific guidance on the Open or an in-state Super Bowl. Value, other attendees, and special circumstances will be taken into consideration.

No: A key vendor offers to take us to an out-of-state Super Bowl. Even if the vendor intends to accompany us, we should decline. Our customers would not view this as a routine business courtesy.

Ask QUESTIONS | **Report** CONCERNS

Honoraria

At the Company, we have a long-standing and recognized heritage of service to our customers and community. There are occasions when a third party asks for Company representatives to make a presentation, participate on a panel or in a focus group, or participate in other such activities related to the work we do for the Company. Compensation for these types of activities is often referred to as an honorarium.

While representing the Company, we must remember that we are acting on behalf of the Company and are responsible for maintaining the Company's heritage and reputation. We do not personally accept honoraria for activities that relate to our duties with, or representation of, the corporation. The honoraria may, however, be accepted by the corporation (as opposed to the employee) and credited to the cost center of the employee participating in the event.

Usually, travel and lodging must be approved by management and paid for by the Company. Conference/seminar fees must also be approved by management and paid for by the Company.

When speaking or presenting at a conference, it is acceptable for conference fees to be waived or reduced if conference fees are waived/reduced for other speakers/presenters at that conference. All other related expenses (travel, lodging, meals) still need to be approved by management and paid for by the Company. Any exceptions need to be approved by management.

An unsolicited donation by the third party that is not delivered to you but is made directly to a bona fide charitable or similar tax-exempt, non-profit, health-related organization is acceptable, but only under all of the following conditions:

- You may not make the donation a condition for your presentation, participation, or other activity
- You may not claim the donation as a deduction for income tax purposes
- You may not be identified to the recipient charitable or non-profit health-related organization in connection with the donation

We may personally accept honoraria for appearances, speeches, or written works that involve outside interests, knowledge, or expertise unrelated to duties with, or representation of, the Company. In such circumstances, we are responsible for all arrangements associated with such honoraria and must perform these activities on personal time.

Offering of Business Courtesies

We may offer a business courtesy to non-government employees and representatives under the following conditions:

- It does not violate any law, regulation, or known policy of the recipient.
- It does not give the appearance of attempting to gain an unfair business advantage or otherwise reflect negatively on the reputation of Company.
- The business courtesy is approved by our management, properly reflected on the books and records of the company, and in accordance with our procurement and reimbursement policies. See your Organization's policies on procurement and petty cash for information on reimbursements; locations to policies can be found in the Appendix.

Exceptions

- We may distribute items, such as pens or coffee mugs, to local health plan customers or potential customers, as long as the value of the items is $10 or less.
- We may not give gifts to union members or union officers.

Further Questions About Business Courtesies?

Contact your Organization's Compliance officer, the compliance department, or the Legal department.

Ask QUESTIONS | Report CONCERNS

Did you know?

There are additional special rules in Section 7 on offering business courtesies to government employees.

Entertainment

Board members, officers, and employees of the Company and its wholly owned subsidiaries may not encourage or solicit entertainment, meals, or recreation ("entertainment") from any company or individual with whom the Company does business. We do not offer or accept entertainment that is intended to gain favor or influence.

From time to time, we may provide or accept entertainment, but only if the entertainment is:

- Reasonable
- Occurs infrequently
- Does not involve lavish expenditures

A representative from each company is expected to attend the entertainment; it may not simply be a gift.

SECTION 7

The Government Is a Unique Customer

We conduct our government business with the highest degree of integrity and honesty.

An important part of our business is the work we do for the government. This includes the Arizona Health Care Cost Containment System (AHCCCS), the Federal Employee Program, and Medicare Part C and D, along with our contracts with state and local government agencies. When we act as a government contractor, we have a duty to the government (along with the public at large) to perform with the highest degree of integrity. In addition, we must comply with not only the letter but also the spirit of the laws and regulations that apply to our government contract business.

Doing business with the government involves unique laws and regulations that do not normally apply to our Commercial business.

The False Claims Act is a federal statute that establishes "liability for certain acts" by any person who "knowingly presents or causes to be presented" a false or fraudulent claim to the government. A false claim is not just the act of submitting a false claim for services to the government. Under this law, a false claim can include any action tied to seeking payment from the government. Violators of the False Claims Act may be required to pay up to three times the amount of damages sustained by the government and may be prohibited from participation in federal healthcare programs.

It is a crime to knowingly:

- Make a false claim for payment from the government
- Make a false statement to the government

Not following laws or regulations may result in criminal prosecution.

If you falsify data submitted to the government, even if you are not attempting to obtain payment, you and the Company may have committed a crime.

You, as an individual, and the Company, as a business, could be subject to:

- Criminal prosecution for the violation
- Large penalties and fines
- Inability to work on government projects in the future

Did you know?

Improperly charging labor or material costs or overhead to the wrong contract, falsifying timecards, or improperly destroying or altering records violates this and other sections of Code Blue.

Do the Right Thing

Follow a policy of full disclosure in negotiations for government contracts or subcontracts, but avoid discussions with anyone outside of AZ Blue's need-to-know group regarding competitive bidding to prevent any allegations of inappropriate insider information and anti-trust violations (see Section 8, Compete Ethically and Fairly).

"Unallowable" costs under government contracts include items such as:

- Advertising
- Public relations
- Donations
- Entertainment
- Fines and penalties
- Lobbying
- Defense of fraud proceedings
- Goodwill

Take special care to seek reimbursement only for allowable costs.

The federal government has special laws and regulations regarding cost accounting and cost charging. The following are examples of situations when you cannot violate Code Blue or the special rules that apply to government contracts.

1. Cost Records, Price Estimates, and Time Charging

We are required to keep and provide the government with access to accounting and other records. This lets the government verify its payments to us for work done on existing contracts. This also helps verify our cost and pricing estimates on future contracts. Therefore, we shall:

- Maintain accurate and truthful records
- Keep records for the period of time required by applicable laws and contract provisions
- Charge all costs and labor accurately, to the appropriate account, regardless of the status of the budget for that account

2. Cost or Pricing Data

We may be required to submit cost or pricing data to the government or to prime contractors. We also may be required to certify that the data is current, accurate, and complete. The definition of which data must be disclosed is very broad. It includes not only hard facts but also management decisions and estimates.

3. Unallowable Costs

We may submit proposals for reimbursement of indirect costs to the government either under cost reimbursement contracts or as part of overhead rates. We will not ask for reimbursement of unallowable costs from government contractors.

Certifications and Representations

Contracts and subcontracts for government projects often require the Company to submit various certifications. These contracts also usually contain clauses that require the Company to certify a variety of matters, such as our compliance with:

- Socioeconomic programs
- Contract specifications
- Environmental laws
- Procurement regulations

All submissions to the government must be accurate and timely and must meet any applicable government healthcare program requirements. All employees who prepare, sign, or in any way support certifications and representations share the responsibility for careful and accurate document preparation.

Although some of the subjects below are discussed more fully in other sections, we must ensure that the Company is in full compliance with the following when dealing with the government:

- Meals and Entertainment.
  Do not offer or give government employees entertainment, including transportation or meals at business meetings, that those employees are prohibited from receiving by their agencies' regulations. Generally, a single meal valued at more than $15 or a number of meals valued at more than $75 are prohibited. It is important to verify the rules applicable to the affected government agency. Also, see Section 12 for guidelines for dealing with elected officials and political candidates.

- Bribes, Kickbacks, and Gratuities.
  Requesting or accepting any of the following from our subcontractors or suppliers when any part of a subcontractor's or supplier's services is charged to a government program is prohibited:
  - Fees
  - Commissions
  - Compensation
  - Gifts
  - Gratuities

Never pay or offer to pay kickbacks to any person or offer or give anything of value to government personnel that creates an appearance that we are seeking to gain special treatment or pay a reward for placing business with the Company.

Did you know?

Because of the significant cost allotted to the Federal Employee Program (FEP), employees who are 100% allocated to FEP are not allowed to accept routine business courtesies from customers, suppliers, or vendors.

Employees who work with Medicare Part C and D products also have special rules about accepting gifts. The Medicare program requires annual reporting of all gifts or entertainment valued at $75 (aggregate value) or more.

The Company may give FEP members and Medicare beneficiaries small novelty items at open enrollments, as long as:

- The value does not exceed $10 (local and FEP) or $15 (Medicare)
- The cost of the items is not charged to the government
- AHCCCS & Part C/D-SNP allow up to $75/member/year tied to health behavior

Code Blue does not allow us to accept or give anything of value to government contractors, employees, and personnel (i.e., FEP, the Veterans Administration).

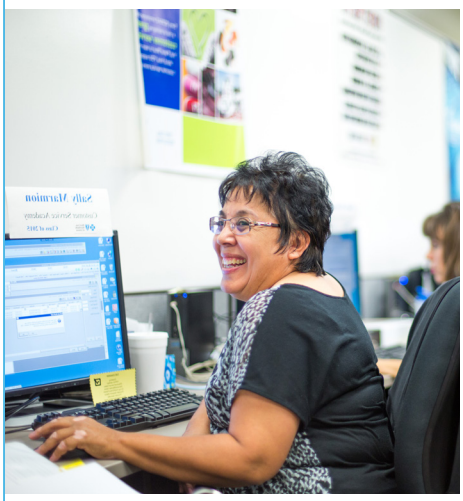
We are not to give anything to union members or union officers.

In addition, local governments such as cities, counties, school districts, or any other local and state government agencies may have special policies regarding conflicts of interest. Therefore, we should ask before providing anything to them. When in doubt, please contact your Organization's compliance officer or Compliance department for clarification.

- **Classified Information and Confidential Data.**
  Do not accept classified government information from any source if you suspect that the release is unauthorized. In addition, do not solicit or accept confidential government information or a competitor's non-public data in connection with any procurement. Federal procurement integrity law specifically prohibits competing companies from seeking or obtaining proprietary information about their competitors during a federal procurement. Therefore, we must never obtain, from any source, federal government information that is procurement-sensitive or unauthorized information about a federal government procurement.
- **Former Government Employees.**
  Special restrictions apply to recruiting former government personnel and the activities of former government employees retained by the Company as employees or consultants. The Legal department must provide clearance before even mentioning possible employment to a current government employee and before retaining any former government employee.
- **Federal Sanction Program.**
  The Company cannot employ or continue employment with anyone who appears on the U.S. Department of Health & Human Services Office of Inspector General's list of individuals and companies excluded from any federal healthcare program. All employees are required to immediately notify the AZ Blue Chief People Officer, Greg Wells, if they are debarred, excluded, or otherwise ineligible to perform work directly or indirectly on federal healthcare programs. This also applies to companies we contract with and vendors of AZ Blue. The Company conducts periodic screenings of the sanction list.

Did you know?

FEP procedures, forms, and a Federal Administrative Manual are available on BlueWeb, the Blue Cross Blue Shield Association's intranet.



SECTION 8

Compete Ethically and Fairly

We inspire health in Arizona as the trusted leader in delivering affordable, innovative healthcare solutions. Not engaging in anti-competitive activities or unfair trade practices is a great reflection of our ethics and values. We are **accountable** and **caring** when we treat others the way we want to be treated. One way to do this is to deal fairly with all of the Company's:

- Customers
- Contractors
- Suppliers
- Providers
- Competitors
- Employees

Our ethical behavior allows us to conduct our business in a manner that maintains a free and competitive market for our goods and services. In turn, we are **accountable** to our customers to improve their quality of life and to provide Arizonans with affordable and innovative health solutions. Furthermore, activities that would prevent a competitive marketplace are against federal laws. Our goal is to compete vigorously with our business competitors on a level playing field.

Circumstances that could jeopardize—or give the appearance of jeopardizing—that goal include:

- Agreements about pricing or other elements of competition (including non-price terms of service, business strategy, or costs) with a competitor
- Agreements to allocate the market for our goods and services among the Company and our competitors
- Agreements among competitors to refuse to deal with particular suppliers or vendors
- Discussions about competitively sensitive information (including pricing, strategy, or supplier relationships) with a competitor
- Bringing non-public information to us from a previous employer

As it is unethical, we do not solicit or obtain confidential information about a competitor in a manner that would be illegal or would require a person to violate a contractual agreement, such as a confidentiality agreement with a prior employer. Do not take advantage of anyone through:

- Manipulation
- Concealment
- Abuse of privileged or confidential information

Finally, all information we provide to our customers and the community at large about our products and services must be truthful and accurate and must not contain misleading or deceptive information.

Did you know?

It's important to be careful when attending gatherings such as trade association meetings and informal events with peers from competitors. Do not get drawn into discussions of inappropriate topics, such as pricing. If you find yourself in such a situation, immediately end the conversation and, if appropriate, ask that your refusal to participate be documented in the meeting minutes. Immediately report any such incident to your Organization's compliance officer as listed in the Appendix.

Ask QUESTIONS | **Report** CONCERNS

SECTION 9

Treat Government Investigations as Serious Matters

Occasionally, the Company may be asked to cooperate with a government investigation or 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. It could also come from a member of an enforcement agency, such as the Federal Bureau of Investigation, the Office of Inspector General, the Department of Justice, or the Arizona Attorney General, to an employee individually.

How Should We Respond?

- When the Company receives official requests for information or cooperation, we notify the appropriate employees of their responsibilities and duties to cooperate and provide such information.
- If you are contacted individually by government investigators and are asked to meet with them individually to discuss activities in connection with your employment, you may do so. 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.
- As the Company may have certain rights and privileges concerning the information you may be asked to provide, you should contact your Organization's compliance officer or the Legal department to let them know you have been contacted.
- If you decide to speak with government investigators, you must be accurate and truthful in all of your answers to their questions. If you are not, you and the Company could be subject to criminal prosecution.

Did you know?

You are free to cooperate individually with government investigators. Before you provide Company documents or data in response to a government request, obtain authorization from your Organization's compliance officer and the Company's Legal department.

The Company will cooperate fully with government fraud investigators and their contractors in any investigation of the company's involvement in the government programs. If any employee other than the compliance officer receives an information request or other inquiry from any fraud investigator, the employee should immediately notify the compliance officer, who will coordinate the company's response to the request. In the compliance officer's absence, the employee may notify any member of the Compliance Committee about the contact from the government investigations.

SECTION 10

Fraud, Waste, and Abuse Prevention, Detection, and Correction

The Company is committed to delivering affordable healthcare solutions to our customers. This is reflected by detecting, correcting, and preventing fraud, waste, and abuse. The efforts undertaken as part of these processes are collaborative in nature and involve training and education, monitoring, audits (including automated claims system checks), the Special Investigations Unit (SIU), and more. All activities are consistent with applicable laws, regulations, and government healthcare program requirements. It is everyone's responsibility to immediately report suspected fraud, waste, or abuse.

The SIU investigates allegations of fraud, waste, and abuse with respect to, but not limited to:

- Any claim submitted to the Company for payment
- Overutilization
- Any scheme to bill for and expect payment when services were not rendered, not received, or misrepresented

Suspected fraud, waste, and abuse for the above circumstances must be reported to your Organization's SIU. Ways to report to the SIU can be found in the Appendix.

Did you know?

Other types of fraud, waste, and abuse, such as internal fraud, waste, and abuse or wrongdoing by employees, can be reported by calling the Compliance Hotline at **1-888-474-3683.** You can remain anonymous. The Compliance Office may work with other areas of the company, such as Internal Audit or Human Resources, when investigating these other types of fraud and abuse. Examples include:

- Misuse of corporate assets
- Financial reporting misrepresentations
- Financial fraud
- Other types of fraud or abuse involving employees' actions

Q&A

Q: I am a customer service representative. I received a call from a member asking for a pharmacy override to fill his prescription early, as the member will be out of the country. Previous customer service records indicate that the member has called on multiple occasions asking for the same override. **What should I do?**

A: Call the Fraud, Waste, and Abuse Hotline as listed in the Appendix.

Q: A staff member from a provider's office calls and tells me they have received an "Explanation of Benefits" and payment for members who are not their patients, yet their physician is listed as the rendering physician. **What should I do?**

A: Transfer the caller to the Fraud, Waste, and Abuse Hotline to report this activity. The SIU will determine if this should also be reported to the Privacy Office as a potential privacy incident.

Q: What are some examples of other types of fraud, waste, and abuse that I should report to the Fraud, Waste, and Abuse Hotline?

A: Examples of other types of fraud, waste, and abuse include:

- Falsification of timecards or other corporate documents
- Inaccurate expense reporting
- Using company assets to run a side or home business (see Section 11 for more information on company assets)

SECTION 11

Safeguard Company Assets

Do not use Company assets or the Company's electronic communication systems for personal reasons, unless corporate policies allow it.

In general, Company assets and electronic communication systems should be used for Company business purposes only. Corporate policy allows use for incidental personal use on a break or lunch hour in certain cases. Using Company assets and electronic communication systems for personal financial gain is prohibited and goes against our values.

Electronic Communications

"Electronic communication systems" include, but are not limited to, the following:

- Electronic mail (email) from the desktop and on mobile devices
- Internet use, including social media such as Facebook, Twitter, YouTube, etc.
- Faxes (over Internet Protocol or analog phone line)
- Voice over Internet Protocol (VoIP)
- Collaboration tools, including instant messaging and video conferencing tools like Microsoft Teams, Zoom, etc.
- Simple Messaging System (SMS)
- Media Messaging System (MMS)
- Secure File Transfer Protocol (SFTP)
- Any other electronic communication method employed by Company

Did you know?

Company assets include:

- Our time
- Office supplies
- Computers
- Telephones
- Copying machines
- Computer software

Please use these assets according to corporate policies, which, in certain cases, may permit incidental personal use on a break or lunch hour or when you receive prior management approval.

For more information on the use of corporate assets, see your Organization's policies on Social Media, IT / Security Violations, and Computer / Internet user agreements as listed in the Appendix.

Do not use company electronic systems for personal use, except as permitted by your Organization's Company Computer and Internet User Responsibility Agreement or policy (signed by employees upon employment) and the Corporate Internet Policies (located in the Employee Guide on the Human Resources page on your Organization's intranet). Do not use company electronic systems to conduct any business other than Company business.

Communicate professionally and respectfully when using the Company's electronic communication systems. This applies to communications with employees, customers, and the public.

By using the Company's electronic communication systems, all employees consent to monitoring at the discretion of the Company.

Did you know?

The Company monitors employees' use of electronic communications consistent with applicable state and federal law. Monitoring is conducted by Company-authorized personnel to protect the Company's legitimate business interests.

Streaming media consumes excessive bandwidth and should be used sparingly and for business purposes. Prohibited use of streaming media includes examples such as sporting events, television shows, and online radio stations.

Visiting websites with inappropriate content is not allowed, even during lunch, breaks, or before/after hours.

SECTION 12

Do Not Speak on Behalf of the Company or Engage in Improper Political Activities

The Company's ability to participate in political activities is controlled by federal, state, and local law. Our Government Relations department and the AZ Blue Legal department must clear all organizational political activity, including use of Company assets, before any engagement in political activity.

The Company strives to promptly respond to press, regulatory agencies, and legislative inquiries with a consistent, factually accurate, and thoroughly researched response. This is particularly important, as many press, regulatory, and legislative issues are contested and can develop into lawsuits. In addition, contacts with the State Legislature, the Congress, and public officials on behalf of the Company are regulated. Both state and federal laws require the Company to register its lobbyists and report its expenditures.

To avoid confusion of AZ Blue's message or inaccurate responses, the Company's officers, directors, and employees shall not respond to press inquiries directly, but will refer all inquiries to the CEO or the public relations' representative designated by the CEO to respond to the press. Refer to CC-001 Reputation Management policy. Similarly, to avoid inadvertent violations of the lobbying laws or confusion over the Company's legislative positions, officers, directors, and employees shall not lobby public officials, state representatives, and senators, or members of Congress on behalf of the Company, unless requested to do so by the CEO.

Do not include political contributions directly or indirectly on expense accounts or in any way that would cause the Company to reimburse for political contributions. If your position with the Company requires you to have personal contact with governmental entities and officials on the company's behalf, be aware of and understand all relevant regulatory provisions regarding such contacts. Make sure that the Government Relations department and the AZ Blue Legal department are aware of your activities because we may be required to register you as a lobbyist and report expenditures.

If you have questions about your actions, get in touch with your Organization's compliance officer or the AZ Blue Legal department before you act.

Did you know?

We are free to participate in the political process on our own time and at our own expense. This means individuals must make it clear that they are speaking or acting on their own behalf.

Do not conduct activities in a way that gives others the impression that you are speaking on behalf of the Company or otherwise representing the Company.

Lobbying is defined by Arizona law as "Attempting to influence the passage or defeat of any legislation by directly communicating with any legislator … or attempting to influence any formal rule making proceeding … by directly communicating with any state officer or employee." A.R.S. § 41-1231(ii)

SECTION 13

Recognize That Our Greatest and Most Valuable Asset Is Our Workforce

The Company is committed to maintaining a safe and professional working environment for all of our employees and ensuring that all employees are treated with fairness, dignity, and respect. We believe in and adhere to treating others the way we want to be treated. See the Appendix for where you can locate your Organization's policies.

To comply with this section, observe all government regulations and rules that protect workplace health and safety. To protect our employees, we take the following steps:

- Security badges must be worn and visible at all times at our corporate campuses.
  - –Employee badges serve as a simple way of instant identification for everyone in the buildings. Our safety increases when Security and employees can tell at a glance who does and does not belong in the building. We must attach badges in a visible location on our clothing or around our neck on a lanyard. Do not attach badges to purses, briefcases, and other items, or put them inside a pocket.
  - –In addition, wearing a badge helps to ensure we don't accidently get locked out of our work area when visiting the restroom or other common areas. This is particularly important when working after standard business hours.
  - –When we forget to bring our badge, we must obtain a temporary badge from the Security/Reception desk in order to work anywhere on campus. This badge will be programmed with our access hours for just one day and must be returned to the Security/Reception desk at the end of the day.
- Visitors must sign in and be escorted while walking around on our corporate campuses.
  - –Visitors cannot freely roam our campus without an escort. Just as important, never let a stranger in our buildings without a valid company-issued visitor badge. Even if we know the person who is visiting, they still need to sign in and have an escort. When approached by a former employee, businessperson, or complete stranger without a badge and escort, direct them to the nearest Security station.
  - –In the case where a consultant has a business associate

Did you know?

The Anti-Harassment Policy covers behavior at the workplace and in any work-related setting outside the workplace, such as during business trips or business-related social events. Harassment includes but is not limited to:

- Offensive comments based on racial or ethnic characteristics of co-workers
- Degrading or humiliating jokes and slurs
- Intimidation of any form
- Unwelcome sexual advances or requests for sexual favors in connection with job decisions
- Offensive (and those perceived as offensive) words, writing, pictures (print and computer images), sounds, electronic mail, text messages, etc., no matter what the source
- Conduct that unreasonably interferes with an employee's work performance or creates an intimidating, hostile, or offensive working environment

agreement (BAA) with us, an access ID card is provided that allows them access to specific areas to the building. An escort is not needed when there is a BAA with the visitor. We can tell when a visitor has a BAA with us when they have an access ID card visible on them. A regular visitor pass is a clip-on laminated paper with that indicates the visitor's name and the name of whom they are visiting.

- Provide a drug-free work environment. All employees shall comply with Company procedures on drug usage and testing. See the Appendix for where you can locate your Organization's policies.
- Provide a workplace that is free of discrimination and harassment based on race, color, national origin, sexual orientation, gender identity or expression, genetic information, religion, age, sex, physical or mental disability, marital status, pregnancy, protected veteran status, or any other classification protected by law.
- Provide employees with important Human Resources policies and other documents which may include employee guides, policies on Equal Employment Opportunity, anti-harassment, compensation, reviews, leave, training, benefits, and other terms, conditions, and privileges of employment.

Inappropriate conduct also includes workplace violence, such as threats of violence or violence directed toward co-workers, or the Company, or "stalking" behavior committed by or directed toward employees.

While on Company work premises (buildings, parking lots, company vehicles), we are prohibited from possessing weapons (including lawfully authorized concealed weapons), explosive devices, or other items that could reasonably be used to harm others. In accordance with state law, a limited exception exists for lawfully transported firearms. These may be kept in private vehicles when the vehicle is locked, and the weapon is stored in a manner that it is not visible from outside the vehicle.

All officers, directors, board members, and employees of the Company and its wholly owned subsidiaries are also prohibited by federal law from continuing employment or service with the company if they have been indicted or convicted on certain types of criminal or misdemeanor charges, on either the state or federal level, without written approval of the Arizona Department of Insurance.

For this reason, all officers, directors, board members, and employees of the Company, and its wholly owned subsidiaries, are required to report any criminal felony charge, indictments, plea agreements, convictions, or violations of insurance law to the AZ Blue Chief People Officer or their Organization's compliance officer within 10 days.

All officers, directors, and employees of the Company and its wholly owned subsidiaries who are required to hold current, active and unrestricted medical credentials, such as MD, RN, PT, and Ph, and have a change in status for that license must report the change immediately to their supervisor and the AZ Blue Chief People Officer.

Board members and officers of the Company must report bankruptcy, receivership, or license revocation proceedings for any business in which they serve as an officer or board member to the CEO or General Counsel within 10 days, to meet state reporting requirements.

Diversity, Equity, & Inclusion Leadership Council

It is essential that we create a culture of inclusion and opportunity as well as actively guard against bias of any kind. Discrimination and racism are real. Our aim is to empower every member of our team to engage in our mission of improving health for Arizonans. We believe that the power and perspective of diversity and inclusion is, in fact, essential to our success in serving our members and customers, achieving our mission, and creating a healthy environment for all.

To support our inclusive culture, the Company has a Diversity, Equity, & Inclusion Leadership Council charged with raising awareness and creating opportunity and change. Council strategic goals include:

- Creating an inclusive environment where every employee feels valued
- Establishing a baseline understanding of diversity, equity, and inclusion throughout the Company workforce
- Fostering a diverse internal and external talent pipeline
- Supporting Company efforts in addressing health disparities

The Diversity, Equity, & Inclusion Leadership Council stands in partnership with stakeholders across the organization to raise awareness and create opportunity for positive change.

Did you know?

If you believe you have been subjected to unlawful discrimination or harassment, you should immediately report the incident to your supervisor, Human Resources, or your Organization's compliance officer.

The Company disciplines anyone who violates Code Blue. This could consist of actions ranging from a verbal warning to dismissal.

We are **accountable** and **caring** when we treat others the way we want to be treated. These are Company values.

Reporting Requirements

Special Reporting Requirements for Management-Level Employees

If a management-level employee is advised of a potential violation of Code Blue, the manager is required to submit this information to either the Compliance Hotline or the compliance officer immediately.

Reporting Requirements for Attorneys

Attorneys for the Company have special reporting obligations. An attorney who suspects material violation of law or breach of fiduciary duty by the Company, an affiliate, or a contractor of the Company shall report it to the General Counsel. If the General Counsel does not take appropriate action or if the General Counsel is directly involved in the violation, the attorney shall report the findings to the Audit, Compliance, and Risk Committee of the Board or the Board of Directors as a whole.

General Reporting Requirements

It is our obligation to know and understand Code Blue. We have an obligation to report all suspected violations of this code to one of the following:

- Your department supervisor, manager, or director, vice president, general manager, senior vice president, or senior manager or above
- Your Organization's compliance officer
- A member of your Organization's Compliance Committee or Compliance department, or the Company's Legal or Human Resources departments
- The Audit, Compliance, and Risk Committee of the board (for financial and audit-related issues) for your Organization
- The Compliance Hotline at **1-888-474-3683** (you can remain anonymous)

Reporting for Contractors, Subcontractors, FDRs, Business Associates, and Other Vendors

Employees of contractors; subcontractors; First-Tier, Downstream, or Related Entities (FDRs); Business Associates; and other vendors may report noncompliance concerns by any of the ways mentioned in Code Blue but can also report through your employer's reporting mechanisms.

Obligation to Report and No Retaliation

We all contribute to an ethical culture for the Company when we report misconduct. When making a report, you will not be required to reveal your name, and if you do, you are protected from retaliation if you make the report in good faith. If you know or should have known of an actual violation of this Code, or any law or regulation and you fail to report it, you will be subject to appropriate discipline, up to and including dismissal.

Code Blue is not a complete list of potential legal or ethical situations you may encounter. It should be liberally interpreted in favor of the highest standards of behavior.

If at any time you have questions about a section in Code Blue and how it applies specifically to your job, be **Curious.** Your Organization's compliance officer, Compliance department, and management will help you determine the right actions to take.

Did you know?

With everyone's help, we can make the Company a place where we are proud to work and a company that is respected in the community for its integrity.

Ask questions and report in good faith without fear of retaliation.

Ask QUESTIONS | **Report** CONCERNS

CODE BLUE APPENDIX: Additional Resources and Contact Information

Blue Cross Blue Shield of Arizona, Trinnovate, Veritage, MediSun	
Chief Compliance and Privacy Officer	Anne.Schrock@azblue.com, 602-864-4315
Staff VP, Corporate & Medicare Compliance and ESG	Veronica.Moore@azblue.com, 602-336-7600
VP, Internal Audit Chief Audit Executive	Deepa.Lohse@azblue.com, 602-864-4520
Sr. Manager, Special Investigations Unit	Michael.Fisher-Mariano@azblue.com
Compliance Department	Compliance@azblue.com
Compliance Hotline	1-888-474-3683
SIU Hotline	1-800-232-2345, ext. 4875, or 602-864-4875
Privacy Department	Privacy@azblue.com
Privacy Hotline	602-864-2255
Record Retention Questions	RecordRetention@azblue.com
Compliance Committee Members	Michele Boggs – Director Organizational & Lead Development Program & Change Kathleen Bonzani – VP Controller & Chief Accounting Officer Colby Bower – VP Provider Network Management Nicole Larson – Director, Medicaid Chief Compliance Officer Scott Mack – VP Group Underwriting Veronica Moore – Director, Corporate & Medicare Compliance Jim Napoli – VP & Chief Pharmacy Officer Erik Ryer – Director Chief Information Security Officer Anne Schrock – Chief Compliance & Privacy Officer Risa Simonis – Risk Manager Chaz Smith – Communications Project Manager, Commercial Segment Lori Turner – SVP Chief Marketing Officer Greg Wells – Chief People Officer See Planet Blue > Our Integrity > What We Do > Compliance and Ethics, for a list of current members of the Compliance Committee.
Employee Guide	See Planet Blue > Employee Central > Human Resources > Employee Guide, Policies, and Procedures
Policies & Procedures	See Planet Blue > MY LINKS > Policy Portal – Archer
IT Service Desk	602-864-4099

CODE BLUE APPENDIX: Additional Resources and Contact Information

Medicaid Segment (Health Choice Arizona)	
Chief Compliance Officer	Nicole.Larson@azblue.com, 480-760-4902
Contract Compliance and Delegated Oversight	Amanda.Pizzolanti@azblue.com, 480-760-4539
Compliance Department email contact info	Compliance@azblue.com
Compliance Hotline (Reporting any compliance issues or concerns including but not limited to Contract Compliance, Fraud, Waste and Abuse (FWA), or Privacy-related issues)	1-888-474-3683
Compliance Committee Members	Michele Boggs – Director Organizational & Lead Development Program & Change Kathleen Bonzani – VP Controller & Chief Accounting Officer Colby Bower – VP Provider Network Management Nicole Larson – Director, Medicaid Chief Compliance Officer Scott Mack – VP Group Underwriting Veronica Moore – Director, Corporate & Medicare Compliance Jim Napoli – VP & Chief Pharmacy Officer David Valenzuela – VP Chief Information Security Officer Anne Schrock – Chief Compliance and Privacy Officer Risa Simonis – Risk Manager Chaz Smith – Communications Project Manager, Commercial Segment Lori Turner – SVP Chief Marketing Officer Greg Wells – Chief People Officer See Planet Blue > Our Integrity > What We Do > Compliance and Ethics, for a list of current members of the Compliance Committee.
Employee Guide	See Planet Blue > Employee Central > Human Resources > Employee Guide, Policies, and Procedures
Policies and Procedures	See Planet Blue > MY LINKS > Policy Portal – Archer
IT Service Desk	602-864-4099

CODE BLUE APPENDIX: Additional Resources and Contact Information

Prosano Health	
Compliance & Privacy Officer	Anne.Schrock@azblue.com, 602-864-4315
Compliance Department email contact info	compliance@azblue.com
Compliance Hotline (Reporting any compliance issues or concerns including, but not limited to, Contract Compliance; Fraud, Waste, and Abuse (FWA); or Privacy-related issues)	1-888-474-3683
Compliance Committee Members	Michele Boggs – Director Organizational & Lead Development Program & Change Kathleen Bonzani – VP Controller & Chief Accounting Officer Colby Bower – VP Provider Network Management Nicole Larson – Director, Medicaid Chief Compliance Officer Scott Mack – VP Group Underwriting Veronica Moore – Director, Corporate & Medicare Compliance Jim Napoli – VP & Chief Pharmacy Officer David Valenzuela – VP Chief Information Security Officer Anne Schrock – Chief Compliance and Privacy Officer Risa Simonis – Risk Manager Chaz Smith – Communications Project Manager, Commercial Segment Lori Turner – SVP Chief Marketing Officer Greg Wells – Chief People Officer See Planet Blue > Our Integrity > What We Do > Compliance and Ethics, for a list of current members of the Compliance Committee.
Policies and Procedures	Intranet Link
IT Service Desk	602-864-4099
Compliance & Privacy Officer	Anne.Schrock@azblue.com, 602-864-4315
Compliance Department email contact info	compliance@azblue.com
Compliance Hotline (Reporting any compliance issues or concerns including, but not limited to, Contract Compliance; Fraud, Waste, and Abuse (FWA); or Privacy-related issues)	1-888-474-3683

1670409-24