



# Federally Required Compliance Requirements

Arkansas Blue Cross Blue Shield and its affiliates is required by the Centers for Medicare and Medicaid Services (CMS)<sup>1</sup>, as well as the federal government, state government and other regulators, to ensure that certain individuals and entities with whom we do business<sup>2</sup> (including healthcare-related professionals and organizations) complete **general compliance training** and **fraud, waste and abuse training** on an annual basis<sup>2</sup> in addition to meeting certain federal and state compliance requirements.

## What Requirements must be met?

**1. Training:** General compliance training and Fraud, Waste and Abuse (FWA) training (where applicable), should be completed annually by **all persons** who have contact (indirect or direct) with beneficiaries of Medicare Advantage (MA) and members covered by the Affordable Care Act (ACA). This includes staff in all billing, reception, lab and clinical areas.

**General compliance training** is required for all persons who meet the criteria above, but certain individuals and entities who participate in the Medicare program are deemed to have met the **FWA** component by virtue of satisfying Medicare's annual certification requirements. This includes entities and/or individuals who are:

- Participating healthcare providers in the federal Medicare program (Parts A and/or B).
- Accredited, Medicare-approved suppliers of durable medical equipment, prosthetics, orthotics and supplies.

---

1. Arkansas Blue Cross and Blue Shield must maintain an annual compliance training program because we are a:

- Contractor with the federal Centers for Medicare & Medicaid Services (CMS)
- Qualified Health Plan (QHP) through the U.S. Department of Health and Human Services (HHS) through the Patient Protection and Affordable Care Act and Health Care and Education Reconciliation Act of 2010 (together referred to as the Affordable Care Act).

2. Entities that must complete annual compliance training (including fraud, waste and abuse training) include:

- First-tier, downstream and related entities (FDRs).
- Delegated entities (DEs).

According to the Federal Register Notice CMS-4124-FC and 45 C.F.R. Subpart D §156.340, providers are considered first-tier and/or delegated entities because there is a direct contract for Medicare/Affordable Care Act Services between Arkansas Blue Cross and each provider.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

## When should training be completed?

The General Compliance Training and/or FWA training must occur within 90 days of initial hiring and annually thereafter. The annual training may be completed at any time during a traditional calendar year. Training must be documented. All documentation is subject to random audit by Arkansas Blue Cross and Blue Shield or the federal government.

In the event that your organization does not provide annual compliance training, Arkansas Blue Cross Blue Shield has made Annual Compliance Training available below. Additionally, Annual Compliance Training is available by selecting the 'Required Annual Compliance Information' link on our website at [www.arkbluecross.com/providers](http://www.arkbluecross.com/providers) under 'Resource Center'.

Additionally, the AHIN User Administrator (AUA) will receive notification, via AHIN, when the attestation is available on AHIN. The AUA should attest that all compliance related requirements have been met by the provider for the plan year. The attestation should be completed by December 31.

**Note:** CMS will be removing the compliance training from the Medicare Learning Network (MLN) website in anticipation of regulation changes for the 2019 plan year. However, if you have already completed the web-based compliance training on the MLN for the 2018 plan year, you are compliant with the requirements for 2018.

### **2. Office of Inspector General (OIG) List of Excluded Individuals and Entities (LEIE), and the U.S. General Services (GSA) System for Award Management (SAM), formerly the Excluded Parties List System (EPLS) , Exclusion Checks**

These lists for individuals or entities excluded by any Federally-funded health care program for participating in or receiving health care reimbursement or payment<sup>3</sup> should be reviewed prior to hiring or contracting and monthly thereafter. Upon discovery of an excluded individual, immediate disclosure must be provided to ABCBS.

---

3. <https://exclusions.oig.hhs.gov/OIG>; <https://sam.gov>





# Annual Compliance Training

## Upholding the Code of Conduct

Our Code of Conduct outlines the standards and rules for ethical business practices for all employees, contractors, subcontractors, providers, first-tier, downstream and related entities (FDRs), delegated entities (DEs) and members. Our company has established a compliance program to oversee adherence to all applicable laws, regulations, company policies and procedures.

As an employee, FDR, DE, contractor, subcontractor, or vendor, you have an important role in supporting the Code of Conduct. You have a responsibility to:

- **Set an example of ethical behavior.**
- **Ask Questions.** Ask your supervisor or a Compliance Officer any questions you may have about the Code of Conduct or any legal issues that you do not understand.
- **Report Violations.** Report actual and potential violations. Pay attention and watch for behavior that could potentially put our company, its assets, fellow employees, subcontractors, or our members at risk.

## Conducting Business Legally and Ethically

We must comply with all applicable state and federal laws, rules, and regulations to avoid large fines or being disallowed to participate in Federal or State health programs or to conduct business in some markets. Our Company seeks to prevent Code of Conduct violations and to avoid legal and ethical issues in several ways including:

- Sound hiring and employment practices
- A written Code of Conduct policy
- A compliance committee.

The Company also has established effective internal controls to promote ethical behavior. Some examples of internal controls include:

### Segregation of Incompatible Duties

- This internal control helps to prevent error and fraud by making sure at least two people work separately to accomplish certain tasks.
- Example: Employees who process claims do not have the ability to enter or change provider information. This minimizes the opportunity to create a fraudulent account and make payments to it.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

## Checks and Balances Procedures

- Checks and balances ensure that no one person or department has absolute control over decisions and clearly defines duties.

Conducting business in an ethical manner means paying close attention to truthfulness and accuracy.

There are many reasons to be truthful and accurate:

- Laws and regulations demand it.
- Our members expect it.
- We need to protect our reputation.

Company employees, FDRs, DEs, subcontractors, providers, and vendors must report and record all information accurately including:

- Any business-related activities on which we must record and/or report data.
- The performance data of both the company and ourselves.
- The amount of time worked.
- Our business expenses.

Employees, FDRs, DEs, contractors, providers, subcontractors, and other vendors who notice or suspect mistakes or falsification of records should report it immediately.

Employees, FDRs, DEs, contractors, providers, subcontractors, and other vendors who falsify information are subject to the full range of disciplinary actions, including termination of employment or contract.

## Copyright and Intellectual Property

Federal law prohibits copying another party's copyrighted work without appropriate permission. Examples of illegal copyright activities include:

- Using copyrighted material in business documents, presentations, and training materials.
- Copying software or installing it without a license, even for business use.
- Distributing or copying copyrighted articles, newsletters, books, and magazines.

## Physical Assets

Personal use of the Company's physical assets is prohibited without approval of your supervisor, even for charitable or professional organizations. This includes:

- Projection and audio-visual equipment
- Copy machines, fax machines, and other office equipment
- Buildings, offices, and meeting rooms



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

- Computer systems
- Supplies
- Furniture
- Software

## Company Time

As with physical assets, any significant use of company time for personal or charitable reasons is prohibited without proper approval.

## Company Records

Employees, contractors, providers, subcontractors, and other delegated entities are required to ensure that company records, including claims and related medical records, are properly protected. Company records include:

- Electronic information such as computer files or email.
- Information stored on any other medium.
- Paper records.

**Note:** Before destroying any company records, verify that a "litigation hold" is not applied to the records. If in doubt, please contact a Compliance Officer with any questions you may have in regard to any "litigation hold".

## Conflicts of Interest

Our Code of Conduct policy defines a conflict of interest as:

"A situation where your personal interests and activities could influence your judgment or decisions."

Examples of a conflict of interest include:

### **Offers of gifts or money**

Accepting gifts for excessive or unusual entertainment that could influence decisions for any conducting business with or seeking to do business with the Company is prohibited.

### **Some secondary employment situations**

Neither you nor members of your immediate family may work or provide services for competitors unless you receive approval from your manager, Vice President, Staff Attorney, or Personnel Director. If you have a second job, be sure to read the Outside Employment Policy and submit an Outside Employment Request Form.

### **Situations where you or family members stand to gain personal benefit.**

You should not engage in transactions or business with third parties that could potentially create financial gain or other benefits that might cause you to favor such third parties at the company's expense.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

Examples might include investing in a medical supply company, working part-time for a provider who does business with the company, or serving on the board of a local hospital. Any such activities would need to be disclosed and approved by the company's Compliance Committee.

Conflict of interest will vary depending on job roles and the specific situation.

For example, working in a volunteer clinic on Saturday may or may not be a conflict of interest for a project manager who works primarily with employees and some vendors. But it could be a conflict of interest for a care coordinator who works directly with members and their medical records.

## Courtesies, Bribes, and Kickbacks

A business courtesy is a gift of low value giving no appearance to an observer that the gift giver seeks improper influence. Business courtesies may be accepted by Company employees, contractors, subcontractors, or delegated entities as long as acceptance of the courtesy does not influence business decisions and the giver is not seeking or working on government related work.

Examples of a business courtesy:

- Low to moderately-valued meals and refreshments at a vendor's expense, in conjunction with a business meeting
- A mug with a supplier's logo
- A promotional T-shirt
- Attendance at a local workshop or seminar at a vendor's expense

**Bribe:** A bribe is an offer of a favor from a potential business partner in exchange for your business. Securing business in this manner is an illegal practice. Usually these incentives are tangible and would be appealing and favorable to you personally, such as payments received for trade secrets or excessive commissions for sales.

Examples of bribes:

- First base tickets to a major league baseball game provided or offered by a potential vendor
- Expensive electronic equipment (e.g., smart phone, tablet, laptop) offered by a customer or vendor

**Kickback:** A kickback is either a payment or goods received in return for purchasing products or services. Often times the kickback is a percent of the value of goods and services where larger purchases result in larger kickbacks. Kickbacks are typically the result of pressure, coercion, or a secret agreement. Because kickbacks are illegal, programs that tie incentives to volume of business (for example, insurance agent commissions) must be reviewed by our Legal Department.

- Examples of Kickbacks:
- Payments made to a group contact in return for awarding business
- Financial incentives provided to physicians for referral of services
- Goods of significant value given to a vendor for reducing their fee



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

## Engaging in Political Activity

Employees, contractors, subcontractors, and other delegated entities should not use Company assets to engage in political activities without prior review and approval. Even incidental or infrequent use is strictly prohibited.

Political contributions by a corporation are restricted by Federal Law. This includes direct and indirect financial support in connection with federal elections. Contributions may be given to candidates for state, legislative and constitutional offices, through a Political Action Committee.

### YOU CANNOT:

- Submit political contributions on expense accounts.
- Allow company assets or resources to be used for a political cause.
- Use company time to support political causes or campaigns.
- Engage in activities that may give the impression that you are representing the company.

## Protecting Confidential and Sensitive Information

There are several ways you can help keep company information safe including:

- Keep confidential information out of sight in your work area.
- Refrain from discussing confidential information with coworkers in public.
- Dispose of confidential and sensitive information in the locked shred bins located in each work area.
- Use a password-protected screen saver.
- Follow the guidelines provided by our Information Privacy and Security program located on the Company website.
- Lock your PC when you are away from your desk.

As a company, we handle a wide variety of confidential and sensitive information including:

- Strategy Information- Information about business strategies and operations that has not been publicly released.
- Negotiations- Information relating to negotiations with employees or third-party organizations.
- PHI- Member information and Protected Health Information (PHI).
- Financial Information- Payment and reimbursement information such as account numbers or non-public financial information.
- PII- Personnel and payroll information such as Personal Identifying Information (PII).

## Harassment and Workplace Violence

Workplace violence is prohibited and includes threats as well as actual physical harm. You cannot bring firearms, weapons, explosive devices or any other dangerous materials to the company's premises. If you are a victim of harassment or if you observe any form of harassment, immediately report the incident to your supervisor, the Director of Human Resources, or a Compliance Officer.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

If you witness a situation in which threats are uttered or someone is physically harmed, report the issue right away. The company understands that these can be sensitive situations that must be addressed with care and confidentiality.

## Fraud, Waste, and Abuse (FWA)

Fraud, Waste and Abuse combined, involves the act of submitting false information either directly or indirectly, that results in unnecessary costs to the healthcare system. Anyone can commit healthcare fraud, waste, or abuse. Fraud can range from individuals acting alone to operations run by groups, institutions and even organized crime.

**Fraud** is defined as anyone knowingly and willfully carrying out, or attempting to scheme or trick to defraud any healthcare benefit program. This could also include obtaining (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any healthcare benefit program.

Some legal definitions of fraud exist and contain different legal elements, such as:

- Intentional deception or deliberate omission
- Knowledge of the falsity of the misrepresentation or ignorance of its truth
- A victim relying on the misstatements
- Damage to the victim
- Wrongful gain to the perpetrator

**Waste** is defined as practices that result in unnecessary costs.

**Abuse** describes practices that, either directly or indirectly, result in unnecessary costs. Abuse includes any practice that is not consistent with the goals of providing patients with services that are medically necessary, meet professionally recognized standards, and priced fairly.

Examples of waste and abuse may include:

- Billing for services that were not medically necessary,
- Charging excessively for services or supplies, and
- Misusing codes on a claim, such as upcoding or unbundling codes.

### Identifying Fraud, Waste & Abuse

As employees, contractors, subcontractors, and delegated entities, it's our responsibility to watch for suspicious activity and potential healthcare fraud.

- Reading your own Personal Health Statement (PHS) is one of the best ways to spot inconsistencies. Are there suspicious expenses?
- Are dates of service documented on the forms correct?
- Were the services billed for actually performed?



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

The most common types of provider fraud typically include:

- Billing for services that were never rendered
- Billing for similar but more expensive services than were actually performed
- Performing services that were not medically necessary in order to bill insurance
- Misrepresenting non-covered services as medically necessary
- Falsifying a patient's diagnosis to justify services performed

Examples of member and employee fraud might include:

- Forging a marriage certificate so significant others can obtain coverage
- Allowing someone to use your health insurance card to obtain medical services
- Leaving adult children on your policy after exceeding the policy's age limit
- Leaving an ex-spouse on a healthcare policy after a divorce is finalized.

### **Reporting Fraud, Waste & Abuse**

If you observe suspicious claims activity or suspect potential claim fraud, do not be concerned about whether it is fraud, waste, or abuse. REPORT IT.

Referrals to the SIU can be made anonymously by:

- Calling 1-800-FRAUD21 (SIU Hotline);
- or Completing the on-line referral form on the company website.

Although not anonymous, you can also refer directly to SIU through the following methods:

- Send an email to [SpecialInvestigation@arkbluecross.com](mailto:SpecialInvestigation@arkbluecross.com)
- Forward information using inner office mail to Special Investigations – 10 South
- Contact SIU staff directly by phone. Contact info can be found on the company website.

When reporting potential Fraud, Waste, and Abuse, provide specific information such as contract numbers, dates of service, provider information, claim information and the nature of the concern or complaint.

- Include any supporting information such as letters, EOB, PHS or claim copies.

## **Working with the Government**

As a participant in government plans and policies, we are expected to maintain programs that reflect an effective and comprehensive approach to compliance. This includes our plan operations and functions performed by our vendors, contractors, and subcontractors commonly referred to as our First Tier, Downstream or Related Entities (FDRs) and Delegated Entities (DEs).

As a government contractor, we must comply with numerous regulations and guidance. Most of those documents can be found on the following websites:

- Centers for Medicare & Medicaid Services (CMS)
- U.S. Department of Health & Human Services (HHS)



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

- Arkansas Insurance Department (AID)

As a part of these government programs, each individual who works on these programs should be aware of the key elements of an effective compliance program.

There are a number of laws, rules, and regulations that apply to healthcare fraud.

Exclusion from Federal Healthcare Programs via the OIG (LEIE), GSA (SAM) Fraudulent practices can result in individuals and businesses being banned (excluded) from participating in federal healthcare programs. These individuals and businesses are reported on national exclusion lists.

#### **Office of Inspector General (OIG):**

The Office of the Inspector General of the Department of Health and Human Services (OIG-HHS) is the largest inspector general's office in the Federal Government, with approximately 1,600 dedicated to combating fraud, waste and abuse and to improving the efficiency of HHS programs.

A majority of OIG's resources goes toward the oversight of Medicare and Medicaid — programs that represent a significant part of the Federal budget and that affect this country's most vulnerable citizens.

OIG's List of Excluded Individuals and Entities (LEIE) is a list of all individuals and entities currently excluded by the OIG. The LEIE is available to the public and can be easily searched using the name of employees or entities.

#### **U.S. General Services (GSA)**

U.S. General Services (GSA) System for Award Management (SAM), formerly the Excluded Parties List System (EPLS): The General Services Administration (GSA) combined the Central Contractor Registration (CCR/FedReg), Online Representations & Certifications Application (ORCA) and the Excluded Parties List System (EPLS) into one main contractor database. This database was named System for Award Management or better known as the SAM registration database. SAM incorporates all government contractor information into one system.

## **Elements of an Effective Compliance Program**

### **Written Policies and Procedures**

Our Code of Conduct sets expectations for our employees and those with whom we work with to understand and comply with all laws, regulations and policies concerning our business.

### **Compliance Officer, Compliance Committee & High Level Oversight**

Our company has a Regulatory Compliance Officer who is responsible for ensuring compliance with government programs and overseeing the Compliance Committee.

### **Effective Training and Education**

Our company understands that the education and training of corporate officers and all employees are significant elements of an effective compliance program.

- According to our policies, all new employees must complete online training within the first week of hire but no later than 90 days of hire and annually thereafter.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

### **Prompt Response to Compliance Issues**

Our company has established and implemented procedures for promptly responding to compliance issues as they are reported. Suspected violations of any part of our government programs or any other type of misconduct will be investigated by the Regulatory Compliance Officer or designee.

### **Disciplinary Action Through Well-Publicized Guidelines**

Upon the conclusion of the investigation of any potential non-compliance, fraud, waste or abuse investigation, the Compliance Officer(s) shall recommend the appropriate corrective and disciplinary actions, which shall be tailored to address the misconduct identified.

### **Internal Monitoring and Auditing**

Our company audit programs include program risk assessments, auditing and monitoring activities and external entity audits from such parties as Centers for Medicare & Medicaid Services (CMS), the Office of Inspector General of the Department of Health and Human Services (OIG-HHS), or the Arkansas Insurance Department (AID).

## **Federal False Claims Act**

### **Federal False Claims Act (FCA) (31 U.S.C. §3729)**

The False Claims Act covers fraud involving any federally-funded contract or program.

Any person who:

- Knowingly presents, or causes to be presented, to an officer or employee of the United States Government or a member of the Armed Forces of the United States a false or fraudulent claim for payment or approval;
- Knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the Government;
- Conspires to defraud the Government by getting a false or fraudulent claim paid or approved by the Government;
- Knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government...

[ . . . ] is liable to the United States Government for a civil penalty of not less than \$5,000 and not more than \$10,000, plus three (3) times the amount of damages which the Government sustains because of the act of that person.

For the purposes of this statute, the terms “**knowing**” and “**knowingly**” mean that a person, with respect to information (1) has actual knowledge of the information; (2) acts in deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information, and no proof of specific intent to defraud is required.

The False Claims Act imposes liability only when the claimant acts “**knowingly**”. However, the Act does not require that the person submitting the claim have actual knowledge that the claim is false. Acting in reckless disregard or in deliberate ignorance of the truth or falsity of the information can also trigger liability.

## **“Qui Tam” Relators or “Whistleblowers”**

The False Claims Act allows private parties to bring an action on behalf of the United States (31 U.S.C. 3730(b)).

The private parties may share in a percentage of the proceeds from the settlement of a false claims act action.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

The FCA provides protection to qui tam relators who are discharged, demoted, suspended, threatened, harassed, or in any other manner discriminated against in the terms of their employment as a result of their involvement in an action under the FCA. This protection is commonly referred to as “whistleblower” protection.

Possible remedies include reinstatement with comparable seniority, two times the amount of any back pay, interest on any back pay, and compensation for any special damages sustained as a result of the discrimination, including reasonable attorneys’ fees.

## Program Fraud Civil Remedies Act

The **Program Fraud Civil Remedies Act (PFCRA)** establishes an administrative remedy against any person who makes, or causes to be made, a false claim or written statement to any of certain federal agencies.

PFCRA gives affected agencies the ability to initiate administrative proceedings on claims of \$150,000 or less when the Department of Justice elects not to pursue False Claims Act remedies for the claims. The Inspector General of the agency investigates the alleged false, fictitious, or fraudulent claims or statements.

The PFCRA provides a person found liable may be required to pay an “assessment” up to double the amount falsely claimed and a penalty up to \$5,000 per false claim or statement. This Act does not create any new civil fraud violations or change the way agencies receive allegations of false claims or false statements. It simply provides an additional legal remedy for false or fraudulent claims.

## Anti-Kickback Statute (AKS)

It is a felony to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce or reward referrals of items or services paid in whole or in part by a federal healthcare program.

Remuneration includes transfer of anything of value, directly or indirectly, overtly or covertly, in cash or in kind.

The key word ‘knowingly’ does not require proof of specific intent to defraud the government. ‘Actual knowledge of the information’ or acting ‘in deliberate ignorance of the truth or falsity of the information’ or ‘in reckless disregard of the truth or falsity of the information’ is enough.

## Physician Self-Referral Statute (Stark Law)

### Physician Self-Referral Statute (Stark Law)

The Physician Self-Referral Statute prohibits a physician from making a referral for certain designated health services to an entity in which the physician (or a member of his or her family) has an ownership or investment interest or with which he or she has a compensation arrangement, unless an exception applies.

## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

### Health Insurance Portability and Accountability Act of 1996 (HIPAA)

This Act contains provisions and rules related to protecting the privacy and security of protected health informations (PHI) as well as provisions related to the prevention of healthcare fraud and abuse.



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

## HIPAA Privacy and Security Rules

The Privacy Rule outlines specific protections for the use and disclosure of PHI. It also grants rights to specific members.

The Security Rule outlines specific protections and safeguards for electronic PHI. If you become aware of a potential breach of protected information, you must comply with the security breach and disclosure provisions under HIPAA and, if applicable, with any business associate agreement.

## Fraud Enforcement and Recovery Act of 2009 (FERA)

The Fraud Enforcement and Recovery Act (FERA) boosts the federal government's power to investigate and prosecute any financial fraud against the government and expands liability under the False Claims Act.

For more information, general compliance or how to report issues, employees can visit Corporate Compliance link on the Company's intranet. Employees, subcontractors, or delegated entities who suspect a violation of the Code of Conduct should promptly report it by contacting a Compliance Officer, through the Ethics and Compliance link provided on website or by calling the Ethics, FWA and Compliance Hotline at 1-877-507-7305.

## Corrective Action

Violations of the Code of Conduct and the Compliance Programs can put the company at risk as well as facing fines, penalties, or losing government contracts.

An employee, subcontractor, or delegated entity that knows of the potential or actual violation and does not report it may face corrective action for failing to report the violation. All suspected violations reported anonymously will remain anonymous. The appropriate disciplinary action is recommended by a compliance officer and implemented in conjunction with the Compliance Department, human resources, and other members of senior management.

## Reporting Violations

Anonymous reports can be made by phone to the Ethics, FWA, and Compliance Hotline. The hotline is operated by a third-party agency that is independent of our company. All reports are reviewed by the company's compliance officers. An employee, contractor, subcontractor, or delegated entity will not be subject to any retaliation for reporting suspected violations of the Code of Conduct or the Compliance Programs and are protected by federal law under the False Claims Act.

Every employee or individual working on the company's behalf, who knows of, or suspects, a violation of our Code of Conduct, is obligated to promptly report it in one of the following ways:

- Talk with your supervisor
- Report anonymously through the Ethics, FWA and Compliance Hotline (1-877-507-7305)
- Report it on the web



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association

- Report to the Regulatory Compliance Officer, who will investigate suspected compliance violations of our government programs:
  - Shirl Welch (501-378-6643 or [smwelch@arkbluecross.com](mailto:smwelch@arkbluecross.com))

## Reporting Harassment

If you are a victim of harassment or if you observe any form of harassment, immediately report the incident to your supervisor, Human Resources, or a Compliance Officer.

## Questions?

If you have any questions regarding the requirements or training, please contact our Regulatory Compliance Office at [regulatorycompliance@arkbluecross.com](mailto:regulatorycompliance@arkbluecross.com).



Arkansas  
**BlueCross BlueShield**

An Independent Licensee of the Blue Cross and Blue Shield Association