Business Conduct & Integrity 2021

for Banner|Aetna

Introduction

When you make a promise, you keep it — like my friend, Mateo. He promised to come over and ride bikes later. We made a pinky swear, so I know he'll be here.

Promises

As a company, we've made promises. What are these promises, and how can we keep them?

Code of Conduct

The Code of Conduct is our promise to act in a certain way. Our promises are grounded in the behaviors outlined in our Fundamentals: The Banner|Aetna Way, These behaviors drive how we approach our business, as well as how we treat each other and the people we serve.

When we follow the Code of Conduct, we keep our promises and exhibit the Banner|Aetna Way by integrating our Fundamentas into everything we do.

We are here to fix healthcare. We make promises, and we keep them — that's our values in action.

Course Overview

We're going to explore how the Code of Conduct covers the promises we make to our constituents and demonstrate the practice of The Banner|Aetna Way Fundamentals. By constituents, we mean members, customers, regulators, providers, shareholders, producers, suppliers, First Tier, Downstream, and Related Entities and other business partners, our associates and everyone in the communities where we work and live.

Promises in Action Overview

Practicing the Fundamentals of The Banner|Aetna Way enable us to act on our promises, which is critical to our ultimate goal as an Arizona based insurance company. So, you'll see some questions that test your understanding of how those Fundamentals result in promises that apply to our business. We call it The Banner|Aetna Way. We'd like to know if we did a good job helping you understand the Fundamentals and promises – so the questions are scored. But the score won't affect whether or not you pass the course. When you finish the course, you'll see that it's complete on your transcript, and you'll see how you did on the questions.

So, let's start looking at those promises.

Our Promises to the Company

Our promises to the company

Fundamental #26 TREASURE, PROTECT, AND PROMOTE OUR REPUTATION

Have a passion for our cause! We're all responsible for, and benefit from, the Banner|Aetna image and reputation. Be a proud brand ambassador for Banner|Aetna

When we practice this Fundamental, we are making these promises:

- Creating a culture of compliance
- Handling conflicts of interest
- Managing records
- Keeping data private
- Keeping information secure

Creating a culture of compliance

Compliance Responsibility

Insurance is a highly regulated business. Following all applicable laws and regulations and behaving ethically – that's how we define compliance. When you do the right thing for the right reason, everyone benefits — members, customers, business partners, plan sponsors, producers, providers, suppliers and regulators.

You, along with everyone at our company, are responsible for creating a culture of compliance. Let's learn how.

Noncompliance Consequences

If you don't act ethically, you put yourself, the company and everyone you work with at risk. Some of the consequences are:

- Harm to members
- Fines and penalties
- Costly corrective action plans
- Disciplinary action
- Damage to the company's reputation
- Loss of business opportunities
- Suspension of operating licenses
- Loss of credibility

Promise #1

Q: Whose job is it to follow all applicable laws and regulations, act ethically and create a culture of integrity?

A. The Chief Executive Officer
B. The Compliance Officer
C. All associates
D. Only associates with **compliance** in their job title

The correct answer is "C". That's right. We're all responsible. When you do the right thing for the right reason, everyone benefits.

Tracking Work Hours

When you keep accurate records, you're following the law. Non-exempt associates

are required to complete timesheets. So, if you're a non-exempt associate, always record all hours you work on your timesheet.

And make sure you get your manager's approval before you work any hours outside of your normal schedule.

Under the Fair Labor Standards Act (FLSA), associates are either exempt or non-exempt. Certain FLSA rules apply to non-exempt associates only. For example, non-exempt associates are required to record all of their time worked, and non–exempt associates are entitled to overtime pay.

Promise #2

Q: I'm a paralegal– and I've been so busy. I want to spend some time tonight organizing my emails and prioritizing my work for tomorrow. Should I record this on my timesheet?

A. Yes
B. No, it's not required. You can choose whether or not you want to record the time.

The correct answer is "A". That's right. When you keep accurate records, you're acting ethically.

Creating a Culture of Integrity

Mistakes can happen. It's impossible to be mistake-free, but you need to own up to your mistakes. And never make a promise if you know you can't keep it. That's integrity in action.

Here are some other ways you can contribute to a culture of integrity:

- Follow all federal, state and local laws that apply to your job.
- Trust your instincts — if something doesn't seem right, look into it.
- If you don't know what to do about a compliance issue, ask your manager or Compliance Officer for help.
- Make compliance a performance and business goal.
- Tell your Compliance Officer and Aetna's Arizona Market Compliance Officer (delegted) about any conflicts of interest. And, report any conflicts of interest in your Code of Conduct Acknowledgement at the end of this course.

Promise #3
Fundamental #5 DO THE RIGHT THING, ALWAYS

Demonstrate an unwavering commitment to doing the right thing in every action and in every decision, especially when no one's looking.

Q: How can I help create a culture of integrity?

A. Hide mistakes.
B. Report known or suspected compliance violations or business conduct and integrity problems.
C. Include compliance measures in performance and business goals.
D. Hope that you can fulfill promises to members, customers and regulators.
E. Contribute to a culture that recognizes compliance as a core competency.
F. Behave ethically.

The correct answers are "B, C, E and F". That's right. That's integrity in action.

Reporting Violations

If you see unethical behavior, report it to your manager or Compliance Officer and Aetna's Arizona Market Compliance Officer (delegted) or use Aetna'a AlertLine ® if you'd rather remain anonymous. Here are some examples of unethical behavior:

- Falsifying records
- Sharing member or other confidential information with someone who doesn't have a business need to know
- Misuse of company time or resources

If you're a manager, be open and fair when someone comes to you with a concern. Help create a trusting environment so associates feel safe.

Promise #4

Q: I just overheard two co-workers talking about making changes to documentation requested in connection with a regulatory audit. I didn't catch the whole conversation. But what I heard sounds wrong. What should I do?

A. Nothing. You're not involved in the audit, so you don't need to speak up.

B. Talk to your manager.
C. Ask Aetna's Arizona Market Compliance Officer (delegted) or your Compliance Officer for help.
D. Share this with a few of your friends and hope that one of them reports it.

The correct answers are "B and C". That's right. If you see or suspect that others are behaving unethically, you have an obligation to report it.

Have Concerns?

It's easy to get help with compliance. Keep reading to learning how.

Contact your manager or Aetna's Arizona Market Compliance Officer

(delegted) or your Compliance Officer to report a concern.

If you want to report anonymously, contact Aetna's (delegated) AlertLine ®. It's available 24 hours a day, seven days a week. Trained staff will gather information from you and an independent investigator will review in order to ensure a thorough investigation.

Please refer to the ***How to Report Compliance and Ethics Concerns*** document or the Ethics line procedure for the Ethics line phone number and mailing address available for reporting concerns.

We strictly forbid intimidation or retaliation against anyone who, in good faith, makes a complaint or reports a compliance violation.

Handling conflicts of Interest

Conflicts of Interest

If you have a relationship with a constituent that affects your ability to conduct business fairly, that could be a conflict of interest. Here are other potential conflicts:

- You work for one of our company's competitors.
- You own — or own part of — a competitor's or constituent's company.
- You get special treatment from a customer or supplier — like a gift, an expensive meal or a discount.

Even if something just looks like a conflict of interest, it could hurt you and the company. Let's look at how you can do business fairly—and win business based on

merit, not favoritism.

Relationships

What if you have a close personal relationship with a supplier the company contracts with? This could be a conflict — even if it's someone in your family who has a relationship with the supplier. You should review all such relationships with your Compliance Officer and disclose them on your Code of Conduct Acknowledgement. The compliance team will help you determine whether you have a conflict and guide you on your next steps.

But what if you're not involved in choosing the supplier? And you don't directly work with them? In this case, even if you have a close personal relationship, it's not a conflict. If you're not sure, or if you think the relationship could give rise to even the appearance of favoritism, contact your Compliance Officer.

Make sure your relationships with our constituents are not conflicts of interest.

Promise #5

Q: I work in the corporate fitness center. My husband is an executive at the company that provides cafeteria services in the corporate office. Is this a conflict of interest?

A. Yes
B. No

The correct answer is "B". That's right. It's not a conflict of interest since you're not involved with the selection of cafeteria vendors.

Significant Ownership Interest

If you have a significant ownership interest in a business*, it can be a conflict of interest.

How much is considered a significant interest? It's when you own one percent or more of the outstanding securities of a business.

*A business that is, or reasonably may become, the company's competitor, customer, or supplier of goods and services — including a partnership or limited liability company.

Promise #6

Q: I know it might be a conflict of interest if I have a significant ownership interest in a company. How much is considered significant?

A. More than one-tenth of one percent
B. One percent or more

The correct answer is ”B”. That’s right. It’s one percent or more.

Gifts

When it comes to giving or receiving business gifts outside the company or company owners, it’s safest not to do either. But if you feel you have to, give nice inexpensive or promotional items.

Don’t give or receive gifts outside the company or company owners worth more than $100.

If you think someone might see your gift as a bribe or an attempt to gain favoritism — even if the gift is inexpensive — don’t give it. Never use a gift to influence a business decision. It’s illegal in many countries, including the U.S.

And it could be against the law to offer any gift, even an inexpensive one, to a government employee. Contact Aetna’ s Arizona Market Compliance Officer (delegated) about government or public sector rules.

Promise #7

Q: I’d like to show my appreciation to a customer. Are any of these gifts appropriate?

A. A case of expensive wine at the holidays
B. A $500 VISA gift card
C. A golf trip for the customer and three friends
D. A 20 person suite to a food/beverage hosted Taylor Swift concert
E. None of the above

The correct answer is “E”. That’s right. None of these gifts are appropriate.

Travel and Lodging

When you travel for business, our company pays your travel expenses. Follow our travel and entertainment reimbursement policies. The customer, supplier or business partner should not pay your travel expenses.

Here's an exception. Let's say a professional organization invites you to deliver the keynote speech at their conference. With your manager's permission, you can accept the event sponsor's offer to pay for your travel and lodging — as long as they offer to pay these costs for the other speakers too.

But never accept payment — like a speaking fee — from the event sponsor. Instead, you can ask them to donate the money — in the event sponsor's name — to a charity.

Promise #8

Q: I'm going to a supplier's headquarters to check out one of their new products. They said they'll cover the cost of my trip. Is that okay?

A. Yes, it's okay for them to cover everything — airfare, hotel, meals and car rental.
B. Yes, but only if they cover the cost of meals and car rental — not hotel and airfare.
C. No, your company should cover the full cost of travel, including airfare, hotel and car rental.

The correct answer is "C". That's right. Your company should pay for your travel costs.

Entertainment

Sometimes you can offer or accept meals or entertainment if it's part of a business meeting. But not if what you're offering or accepting is lavish or very expensive. For example, a round of golf with a business associate may be okay. A paid vacation for themselves and their family at a golf resort is not okay.

Lavish entertainment may look like a bribe. You don't want expensive gifts to influence your business decisions. It's important that you do business fairly and legally. Reach out to Aetna' s Arizona Market Compliance Officer (delegated) if you have questions.

Promise #9

Q: We need to create a new app. My team got some bids, but we haven't selected a company yet. An account rep from one of the bidding companies invited me to an all-expense paid golf weekend at Pebble Beach. It sounds like fun. Should I go?

A. Yes
B. No

The correct answer is "B". That's right. You don't want lavish entertainment to influence your business decisions.

Public Sector Employees

When we deal with government employees or public officials, there are special rules for gifts, travel and entertainment. The rules vary by state. So always check with Aetna's Arizona Market Compliance Officer (delegted) before any exchange of gifts, travel or entertainment with the public sector.

The rules are very restrictive, so you must get approval before you take action. There are no exceptions.

Promise #10

Q: I'm stuck at the airport, and I bump into Rob. He's an HR rep for a municipal customer I've been trying to re-sign. We both have time before our flights, so I want to take advantage of this stroke of good luck. I invite Rob to a restaurant at the airport. I let him know that I'm picking up the tab. Is this okay?

A. Yes, as long as the cost of Rob's meal isn't more than $50.
B. No, because Rob is a government employee, you can't offer anything to him—including gifts, meals or entertainment.
C. Maybe. You should contact Aetna's Arizona Market Compliance Officer (delegated) FIRST to see if it's okay, based on government gift rules.

The correct answer is "C". That's right. Contact Aetna's Arizona Market Compliance Officer (delegated) first, before you offer the meal.

Have Concerns?

It's easy to get help with conflicts of interest. Here are some tips and resources:

Contact your Compliance Officer, Aetna's Arizona Market Compliance Officer (delegated) or talk to your manager if you think there's a conflict of interest. Disclose any potential conflicts of interest on your Code of Conduct Acknowledgement.

For the public sector, always check with Aetna's Arizona Market Compliance Officer (delegated) first, before you give or receive a gift. And check before you offer or accept meals or entertainment.

Managing records

Records Management

Records management starts with you. When you create, store or destroy business records, do it the right way. Follow our records retention process. If you don't, we could be exposed to some serious risks:

- High costs: Storing expired records is expensive.
- Lengthy lawsuits: Business records are discoverable. This means they can be used in a lawsuit. Expired records can increase our company's legal costs and harm our case.
- Penalties: Mishandling records can lead to fines from government or regulatory agencies. Our records retention and destruction policies require that we keep records as long as necessary to comply with all legal requirements.
- Damaged reputation: Our company loses credibility when we mishandle records.

If you're not sure about records management, know where to get help.
The Code of Conduct shows us how to manage records safely. Let's look at how we can keep our promise to the company.

Record Types

A business record is anything written or recorded that has lasting value for the company and has to be kept for business, legal or regulatory reasons. Some examples are meeting minutes, tax or financial transactions, compensation data and training records.

Business records can be in any format that someone can retrieve or distribute:

- Paper documents
- Emails
- Voicemails
- Audio or video recordings
- Images
- Web or blog postings
- Or data on a computer or thumb drive

Any business record can be part of a lawsuit, audit or investigation.

Always be careful when you create a business record. If you wouldn't want to see it on the front page of a newspaper, don't create it. Ask yourself:

- Is a written message necessary?
- What's the business need for this record?
- Is a phone call or face-to-face meeting enough?

Promise #11

Q: I know I need to be careful with business records. Which of these is considered a business record?

A. Paper documents
B. Audio or video recordings
C. Voicemails
D. Emails
E. Electronic images
F. Web sites and content posted to company websites
G. Thumb drives

The correct answers are "A, B, C, D, E, F, G". That's right. Business records come in any retrievable form.

Record Storage

You only need to keep one copy of a business record. So if your coworker emailed meeting notes to your team, you don't need to keep your handwritten notes. A duplicate record is disposable — you may destroy it.

Store electronic business records in a central location identified by your manager.

Don't store them on your computer hard drive, in your inbox or in your personal folders.

Label all stored files so you can clearly see the contents and date range. Make sure you can easily access active business records. Only send inactive records to offsite storage.

Promise #12

Q: Sue and I went to a quarterly meeting, and we both took notes. After the meeting, Sue emailed her notes to our team. Her notes are now considered the business record for that meeting. What should I do with the notes I took? What should Sue do with her written notes?

A. Keep a paper copy of your notes at your desk. Sue should also keep hers as a backup.
B. Send your notes to offsite storage. Sue can also send hers to offsite storage or keep the notes in a locked drawer at her desk.
C. Destroy both. Meeting notes aren't business records.
D. Sue's notes are a business record — she should store them in a central location identified by your department. Your meeting notes are a duplicate. You may destroy them.

The correct answer is "D". That's right. Your notes are a duplicate, so you can destroy them. Sue should store her notes in a central location – not offsite – because hers are an active business record.

Sending Records

When you send a business record, only send it to the people who need it. Ask yourself three questions:

- Who should get it? Don't automatically Reply All or send information to an entire workgroup if they don't need it.
- Does it need a label? If you send confidential or proprietary information, label it "For Internal Use Only".
    - Remember, even if you mark it "For Internal Use Only," your communication is still discoverable in a lawsuit.
- Is security a concern? Don't send confidential data, such as birthdates, Social Security numbers, or personal health information unless there is a business

need.

- Contact the person requesting the confidential data. Find out why they need it.
- Make sure it stays secure; send securely via email, or use a secure fax machine or the U.S. Postal Service (rather than interoffice mail, which might be seen by someone other than the intended recipient).

Promise #13

Q: I have the final document for a claim appeal. My boss asked me to get it to the right place, but I'm not sure exactly who should get it. What should I do?

A. Send the record only to the team handling the appeal.
B. Send the record to the entire department — someone will know where it should go.
C. Send the record only to your boss. Let her decide how to handle this.
D. Send a copy of the record to your home email account. You can review it later and then decide how to handle it.

The correct answer is "A". That's right. Only send the record to those who need it.

Legal Hold

A Legal Hold Notice is an email communication that tells associates what business records they need to keep for a legal matter.

If you get a Legal Hold Notice:

- Follow all instructions. The notice tells you what records you must keep and for how long.
- Don't follow the records retention process for these records. The Legal Hold Notice takes precedence.
- Don't destroy the records. Even during Annual Records Cleanup, preserve all records related to a legal hold.
- Click on the acknowledgment link in the notice. Answer the questions that follow.
- If you send the records to offsite storage, apply the record code that's in the notice.
- And finally, if you have questions, contact the attorney or paralegal who issued the notice.

When the legal matter ends, you'll get a Legal Hold Notice Termination email. Then you can manage the records as you normally would. Remove the hold code for any records stored offsite.

If you ignore a Legal Hold Notice or destroy records protected by a legal hold, you and the company face serious consequences — disciplinary action, fines and court-ordered sanctions.

Promise #14

Q: A customer filed a lawsuit against our company. I received a Legal Hold Notice; we have some documents that might hurt my company's defense. What should I do?

A. Shred the documents.
B. Contact the attorney or paralegal who issued the Legal Hold Notice.
C. Dispose of the documents according to the records retention process.

The correct answer is "B". That's right. Complying with a Legal Hold Notice is serious. If you have questions, contact the attorney or paralegal who issued the notice.

Destroying Records

When you have storage questions, check the company's procedure. And when it's time to destroy a business record, remember:

- Don't use public trash cans or dumpsters.
- Don't destroy records that are part of a legal hold.
- Use secure shredding bins for papers, compact discs, videotapes and thumb drives.
- Protect business records when you move. If you're changing desks or offices, relocate or destroy the files in your office space as appropriate.
- If you're a teleworker, use your home office shredder; or go to your nearest office location and use the secure shredding bin.

Promise #15

Q: I just learned about business records and disposable records in my team meeting. When I got back to my desk, I realized some of my emails are business records.

How should I store them?

A. Check the company's storage and destruction procedures.
B. Keep storing the emails in your inbox according to the records retention process.
C. Print copies of the emails and send them to offsite storage.

The correct answer is "A". That's right. When you have storage questions, check the company's procedures.

Keeping data private

Privacy

Our members trust you with confidential data. Protect it as if it were your own. Follow any local, state, and federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA). If you work in another country, you'll need to follow other laws such as the European Union Data Protection Directive or the General Data Protection Regulation (GDPR), effective in May 2018. In fact, you and the company face penalties when you don't follow the laws.

But just being in compliance with privacy laws isn't always enough. You may work with data that isn't covered by today's privacy laws, such as information about consumer purchasing habits or history. You need to collect, use and protect all consumer and member confidential data respectfully. Consider what the consumer or member would expect of us.

When you protect and respect confidential data, you earn the trust of everyone you do business with. Let's see how you can keep your promise to the company and to the people you serve.

What is Protected Health Information?

One type of confidential data is Protected Health Information (PHI). According to HIPAA, PHI is any data that identifies a person and relates to their physical or mental health. It's also data that relates to the delivery or payment of the person's health care. PHI includes:

- Demographic data – a member's name, address, telephone number, Social Security number, and date of birth

- Insurance status – a member's enrollment, termination, ID card and coverage status
- Data related to claims – date of service, claim description, provider name, amount paid, procedure name, diagnosis information
- Other pharmacy claim data – prescription number, drug name and pharmacy name
- Financial data related to a Flexible Spending Account (FSA), a Health Spending Account (HSA) or a Health Reimbursement Arrangement (HRA)

In addition to PHI, you need to protect other information that can identify individuals. This includes employment data and information collected through our websites or mobile devices.

Handling Protected Health Information

Be careful when you work with PHI. You need to comply with HIPAA and the company's privacy policies whether you use or share data internally, or send it outside of the company*.

You can generally use or share PHI for health care operations or for payment purposes. You can also share PHI with providers for treatment purposes. It's important to know why someone is asking you for PHI, and that you only send the minimum data needed to do the job. For example, most of the time, you don't need to give out Social Security numbers, even if the data is staying internal.

So protect the confidential data you handle in your job. Never share it with friends or family, and never email it to your personal email account.

*Always check the company's policies and procedures, or check with your manager or Aetna (delegated) Privacy Consultant if you have any doubt about whether to send PHI.

Promise #16

Q: Someone asked me for a list of members who had claims last month. He wants names, Social Security numbers, birthdates, dates of service and provider names. I'm not sure I should share all this. What should I do?

A. Find out why he needs the data.
B. Ask if he needs Social Security numbers in order to do his job.

C. Find out if he needs all of the data to do his job.
D. None of the above. Since the request is internal, HIPAA and the company's privacy policies don't apply.

The correct answers are "A, B and C". That's right. HIPAA and the company's privacy policies apply when you're sending data internally or externally.

Privacy Resources

You have a lot of resources to help you protect member information. Make sure you read the company privacy and information security policies.

Check with your manager or Aetna (delegated) Privacy Consultant to make sure you have all the privacy training needed for your job.

Contact the Privacy Office whenever you have a question about privacy. Shannon Wood currently support Banner|Aetna for privacy. She may be reached at woodshannone@aetna.com

Promise #17

Q: My manager asked me to format an Excel spreadsheet for a mailing – it has member names, addresses and ID numbers. I need to send it to our supplier by 4:00 today. I'm not good with Excel, but my spouse is a whiz. She promises to delete the file as soon as she's done formatting it. I trust that she won't share it with anyone. Can I send it to her?

A. Yes
B. No

The correct answer is "B". That's right. Don't send it. If you're not sure what to do, contact the Privacy Office.

Handling a Potential Privacy Breach

If you find out about a potential privacy breach, contact the Privacy Office and your supervisor immediately. It's important that you act quickly. In some cases, we have to notify regulatory agencies or members who were affected by the breach.

Promise #18

Q: I'm in a rush to email enrollment files to a plan sponsor. I'm sending the contact person the list of names, addresses, birthdates and Social Security numbers. Then I

noticed that I sent it to the wrong plan sponsor. What should I do now?

A. Call HR to report the incident.
B. Recall the message to stop the person from seeing the email.
C. Quickly send an email to the person you sent the file to. Explain the error and ask him to delete the email.
D. Contact the Privacy Office immediately.
E. Report it to your manager.

The correct answers are "D and E". That's right. If you suspect there was a privacy breach, the Privacy Office needs to act quickly to investigate it.

Suppliers and Confidential Information

We have to protect all individually identifiable information – Protected Health Information, Social Security numbers, and any other data we have related to a member, associate or customer. But there's other confidential data we have to protect:

- Business plans or customer lists
- Data about job applicants, current associates, former associates, customers, providers, suppliers, consultants and business partners
- Information owned by a third party that we use through a licensing agreement

If you work with suppliers who have access to any of this information, these suppliers need special oversight. Always check with Procurement. They'll make sure the proper contract terms are in place.

Promise #19

Q: My team wants to create a communication for members and we want to distribute it as soon as possible prior to their renewal date. Will our Marketing Director be the right contact to confirm the print vendor is approved?

A. Yes
B. No

The correct answer is "A". Our Marketing Director will ensure that all vendors used for print and fulfilment have been approved. We should not use such vendors without confirming, as these communications often contain PHI.

Have Concerns?

It's easy to get help with privacy concerns. Here are some tips and resources:

The Privacy Office is your first point of contact for all of your privacy questions.

Contact the Aetna (delegated) Privacy Office and your manager right away when you find out about a breach.

Review the company's Privacy policies to learn more.

Keeping information secure

Risks

There's valuable data in your computer and workspace. When you protect this information from inappropriate access, use or disclosure, you prevent serious risks. Here are some of the dangers:

- Information ending up in the hands of the wrong person. Criminals or hackers might steal members' identities. Our rivals might get a competitive advantage.
- Inaccurate information. Customers may lose faith or think we deliver poor service.
- Lost information. We have to spend time and money to recreate it.

You handle company information every day, so you're our most important line of defense. The Code of Conduct shows us how to protect our members, customers and our company. Let's look some highlights from the Code.

Access Control

Your access to information depends on your job role. Our company manages your access based on risk. We limit access to high-risk data, such as Social Security numbers. You'll only get access to high-risk data if you need it to do your job. We call this process "access control."

To improve access controls, here are some actions you can take:

- Verify the level of access before you approve. If you're responsible for reviewing and approving access, make sure you're verifying that the level of access is appropriate for the associate's role and job function.

- Remove your access when you no longer need it to do your job. When you transfer within the company to a different department or to a different job function, you and your manager must review your access. If your new job role doesn't require access to high-risk data, work with your manager to remove your access, when applicable.

Physical Data Security

Just as you protect electronic data, protect your physical workspace too. Keep hard copy files safe – lock them up when you're not there. Shred documents before you throw them away. You'll stop criminals from stealing information from the trash.

Be aware of your surroundings. When you discuss or display confidential information, make sure no one can overhear or see it. If someone without a badge approaches you, direct them to Security.

If your office location does not utilize badges, report suspicious activities to security or local law enforcement officials.

Company Information

Some company information is for internal use only. When you attend meetings, protect this information. Don't share it without permission.

Our company monitors online and social media comments. If you inappropriately share internal company information, even on your own time, you could face disciplinary action. You could even lose your job.

Promise #20

Q: I was in an internal company meeting. The CEO talked about how great our stock is doing! During the meeting, I Tweeted something the CEO said. I included a picture of the graph that shows the increase in the stock price. Was that ok?

A. Yes. The stock price was public information.
B. No. Information from internal meetings is confidential.

The correct answer is "No". That's right. Internal meeting information is confidential.

Passwords

Use a strong password to keep company, customer and member information secure. A strong password includes upper and lower case letters, numbers and special characters. And it has to be at least eight characters long.

Here are some other ways to keep your password strong:

- Don't use passwords that others can guess such as your name, hobby or birthdate.
- Keep your password private, even from friends, assistants or colleagues.
- Don't write your password down. Instead, consider using a multi factor sign-on or password manager.
- Keep your company user IDs and passwords separate from your personal ones.

Promise #21

Q: I know I need a strong password. Which one would be best?

A. johnsmith29
B. 20A3tn@10
C. Golfguy1
D. Bluetoothl

The correct answer is "B". That's right. That's a strong password. It has the correct combination of letters, numbers and characters. And it's hard for someone to guess.

Criminal Activity

Criminals can be creative in how they try to steal associate and member data from you. Here are some ways you can protect yourself and the company from fraud, identity theft and computer network disruption:

- Confirm the person's identity. If someone asks you for confidential data, even if it seems legitimate, check with your manager before you send it.
- If you get a phone call from someone who claims to work at our company, check the address book. If the person isn't listed, politely end the call.
    - If someone is listed, either call or email them to confirm their identity.
- Immediately delete any suspicious emails. Don't click on attachments or links

if you don't know the sender.

Phishing

Phishing is a very aggressive attempt to entice an individual to click on a link or open an attached document in an email in order to gain access to confidential information.

These emails can be very convincing and generally appear to be coming from legitimate sources. Most of these emails are personalized with your information such as name, title and address that is easy to find on social media or company websites. Phishers also like to use scare tactics to pressure you to submit confidential data, click a link or open an attachment. Don't be fooled! A best practice is to delete the email if you do not know the sender.

Here are some ways to avoid falling prey to phishers:

- NEVER open the attachment or click a link
- NEVER enter a password
- NEVER forward the email
- Look for grammatical errors in the email

Vishing

Vishing is short for Voice Phishing. With Vishing, the criminal or scammer will attempt to get financial or personal information by calling the victim on the phone. Vishers have become more sophisticated in recent years by misrepresenting the phone number from which they are calling so it appears to be coming from a trusted source. They have been known to use background noise to mimic a legitimate call center, and they can even hold the line so when you attempt to call back, you will be put right back in touch with them. If the call seems suspicious or too good to be true, hang up. Here are some ways you can keep safe:

- Never provide password, PIN or personal information over the phone.
- Never give bank or credit card information over the phone
- If you get a call regarding bank or credit card information, hang up and call the number on your bank statement or credit card from a different phone (if possible)
- Beware when being asked for "verification" information such as name, address, account or phone numbers associated with accounts or services

Promise #22

Q: I work with confidential data a lot. How can I protect confidential data from criminals?

A. If someone asks you for confidential data, even if it seems legitimate, contact your manager or support services before sending.
B. If you get a phone call from someone who claims to work at our company, check the address book. If the person isn't listed, politely end the call.
C. Don't open unfamiliar emails, attachments or links.
D. If an unfamiliar person asks to be let in, direct them to Security.
E. Use a shredder to destroy disposable records containing confidential data.

The correct answers are "A, B, C, D and E". That's right. These are all ways you can stop criminals and keep your promise to the company.

Promise #23

Q: Do you know which of these incidents actually happened?

Incident #1

Associates received an email that appeared to be from a major bank. The bank told recipients that they were part of an audit, so they need to verify certain information. The email stated the request is "in accordance with the bank's existing contract" with our company. Several associates gave the bank personal information such as their user ID numbers and the last four digits of their Social Security numbers.

Incident #2

Associates received an email that appeared to be from a business unit within our company. The email asked the associates to verify their employment status so they could keep their access to a customer's website. Several associates gave their names, years of service, company ID numbers and their manager's name and ID number.

The correct answers are "#1 and #2". That's right. Both incidents happened at a major corporation. Keep our company safe. Always verify the identity of the person, company or department before providing confidential information.

Company Equipment

Someone may steal your laptop from your office, home or car. It's an easy way for thieves to steal personal, member and company information. When you're not using your laptop, lock it in a filing cabinet or drawer.

Here's how you can keep your laptop safe when you're in a public place:

- If you're in a restaurant, keep your laptop in sight.
    - If you must set it down, loop the strap around your chair leg to prevent a thief from grabbing it.
    - If you can't keep your laptop in sight at all times, lock it in your car trunk before you drive to the restaurant. Do it before you get there so no one near the restaurant can see.
- If you're in a taxi, train or bus, keep it on your lap. Never put your laptop in the trunk of a taxi.
- If you're on an airplane, put your laptop under the seat in front of you – not in an overhead bin. Never check your laptop as baggage.
- If you're at a hotel, lock your laptop in the room safe or hotel safe. If neither is available, use your cable lock to secure the laptop to a non-moveable object in the room.

Promise #25

Q: I'm meeting a broker for dinner right after work. The restaurant is on my way home, so I'll have my laptop with me. How can I make sure nobody steals it?

A. Bring it into the restaurant with you and check it at the coat check window.
B. Bring it into the restaurant with you and loop the strap around the leg of your chair.
C. Hide it in the back seat of your car and cover it with a blanket.
D. Lock it in the trunk of your car before you get to the restaurant.

The correct answers are "B and D". That's right. Loop the strap around your chair leg or lock it in your trunk before you get there. These are the best ways to keep your laptop safe.

Social Media

You're free to express your opinions on social media on your own time and on your own computer. But at the same time, you also must protect our company. If

your audience knows you're employed with our company, always be clear that your opinions are your own and not our company's.

Never include your job title or function on your social media profile. If cyber criminals find out where you work and what kind of work you do, they may target you.

LinkedIn is the only social media site where you may include your job title and company name on your profile.

Promise #26

Q: Last night, I saw some politically charged posts on my newsfeed. People were arguing about state-run Insurance Exchanges. One of the posts was from someone I work with. She identified herself as an associate and stated her opinion. Was this okay?

A. Yes, as long as she identified herself as an associate, she could say whatever she wanted.
B. No, we forbid associates from identifying their affiliation with our company on social media sites.
C. Maybe, as long as she was clear that her opinions were her own – not the company's.
D. Yes, associates should identify their company affiliation on all social media sites.

The correct answer is "C". That's right. This might have been okay if she clearly stated that her opinions were personal and not the company's.

Have Concerns?

It's easy to get help with security concerns. Here are some tips and resources:

If you lose your laptop, contact support services and let your manager know immediately. If you are worried about building security or safety, contact local Security or law enforcement. If someone asks you for confidential data, even if it seems legitimate, contact your manager, IT Support or Aetna's Arizona Market Compliance Officer (delegted) before sending the information.

Our Promises to One Another

Our promises to one another

Treating each other – and everyone with whom we do business – with respect

Treating each other – and everyone with whom we do business – with respect. It's a key behavior of the *Banner|Aetna Way!*

Fundamental #23 FOSTER HEALTHY RELATIONSHIPS

Get to know our customers, partners, and co-workers on a more personal level. Treat everyone with the dignity and respect they deserve. Talk more and e-mail less.

Respect and Collaboration in the Workplace

We all deserve to work in a place that's fair and where we feel respected. You can help create a safe and inclusive workplace free from discrimination, intimidation, harassment and retaliation.

Whenever you interact with coworkers, treat them with fairness and respect. This shows that you value diversity of cultures and ideas.

When we have this kind of workplace and we work together, we get great results.

The Code of Conduct helps us promote an inclusive work environment. It also has ways to report your concerns when you believe something's not right.

Let's look at a few examples.

Harassment-free Workplace

When you're with co-workers — no matter where you are — show that you value your work relationships.

If you see behavior that's intimidating, hostile, or offensive, it's your responsibility to help stop it.

Promise #27

Q: My colleagues and I are at a restaurant, winding down after a stressful week at the office. Lots of jokes and stories ae being shared, but the tone is getting increasingly off-color. I know the jokes are "crossing a line." What should I do? (There's more than one correct answer.)

A. Laugh along with everyone else.
B. Don't participate; walk away and just let it go. You're the only person who seems to object.
C. Say, "Hey, I think we're getting carried away. We don't want to offend anyone."
D. Discuss it with your manager or call HR.

The correct answers are "C and/or D". That's right. Ask your co-workers to stop, or discuss it with your manager or HR. No matter where you are, try to stop offensive behavior. Make sure your actions promote a respectful workplace.

Fair Employment Practices

We want our employment practices to be fair, and we want to avoid even the appearance of favoritism in the workplace. So, people with close personal relationships must not be in supervisory or subordinate reporting relationships, or other positions of authority that can influence employment decisions.

If you believe that a close personal relationship involving you or others could affect the workplace, it's your responsibility to raise the issue. Talk with your manager or report your concerns to HR or Ethics Line.

Promise #28

Q: My manager reports to my husband's best friend. Should I do something? (There's more than one correct answer.)

A. Talk to your manager about it.
B. Don't do anything — it's his best friend, not a relative.
C. Call HR.
D. Call Ethics Line to anonymously report the situation.

The correct answers are "A, C, and/or D". That's right. If you're concerned about a relationship that could affect the workplace, tell your manager, CEO or call Aetna's

(delegated) AlertLine ®.

Respect for those with whom we do business

All interactions with our constituents—members, customers, providers and other business partners should be respectful and responsive to the diverse needs of the people we serve.

We do not unlawfully discriminate, exclude or treat people differently based on their race, color, national origin, sex, age, or disability.

We offer accommodations to individuals with disabilities and individuals with limited-English proficiency.

To learn more about nondiscrimination and the final rules for Section 1557 Nondiscriminatory Provision of the ACA, contact Aetna' s Arizona Market Compliance Officer (delegted).

If you receive a complaint of alleged discrimination from one of our members or someone else, have concerns about possible discrimination against one of our members or someone else, or feel that you, as a member, have been discriminated against, there are **resources** dedicated to assisting you.

Commercial

Civil Rights Coordinator
Address: P.O. Box 14462, Lexington, KY 40512 (CA HMO customers: PO Box 24030 Fresno, CA 93779) Phone: 1-800-648-7817, TTY: 711 Fax: 859-425-3379 (CA HMO customers: 860-262-7705) Email: CRCoordinator@aetna.com

Have Concerns?

If you see behavior that doesn't line up with our promises, speak up. Talk to your manager, CEO, or someone from Human Resources. Keep reading to find out more.

If you raise a concern, we appreciate it. We don't allow intimidation or retaliation against anyone who, in good faith:

- Makes a complaint or reports a violation internally or to any law enforcement or government agency
- Cooperates or helps with a government or internal investigation

- Conducts self-evaluations, audits, remedial actions or other activities in support of our compliance program
- Provides information to the government or internally about a breach of law or company policy

If you would rather report your concern anonymously, call the Aetna (delegated) AlertLine ®.

We strictly forbid intimidation or retaliation against anyone who, in good faith, makes a complaint or reports a compliance violation.

Our Promises to Conduct Business Fairly

Our promises to conduct business fairly

Preventing fraud, waste and abuse

Handling suppliers

Preventing fraud, waste and abuse

Education Requirements

Every year, millions of dollars are spent because of fraud, waste and abuse. You can help lower the cost of health care by learning how to prevent fraud, waste and abuse. That's why this training is required within 90 days of when you're hired or contracted, and every year after that.

Who requires this training? Several state insurance departments, the Office of Personnel Management-Office of Inspector General (OPM-OIG) and the Centers for Medicare & Medicaid Services (CMS).

Let's see how preventing fraud, waste and abuse can help you keep your promise to conduct business fairly.

Fraud, Waste and Abuse

Everyone —associates, executives, contractors, subcontractors and business partners — is responsible for preventing and reporting noncompliance and fraud, waste and abuse. When you recognize what fraud, waste and abuse is, you can help

stop it.

Fraud is intentionally submitting false information for money or some other benefit. If a doctor bills for a service she didn't perform, that's fraud.

Waste is the overuse or careless use of health care services. It causes unnecessary costs and a misuse of resources. If a doctor refers a member for numerous tests when one test would be sufficient, that's waste.

Abuse is any action that may result in improper payment, unnecessary costs or items and services being provided that aren't medically necessary. If a pharmacy bills for a brand name drug when a generic was dispensed, that's abuse.

Intent and knowledge make the difference. With fraud, there is intent to get some benefit or payment for yourself and the knowledge that what you're doing is wrong. Waste and abuse don't require the same intent and knowledge.

Fraud

CMS defines fraud as knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program or to obtain (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 health care benefit program.

Waste

CMS defines waste as the overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

Abuse

CMS defines abuse as actions that may, directly or indirectly, result in: unnecessary costs to the Medicare Program, improper payment, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary. Abuse involves payment for items or services when there is no legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment. Abuse cannot be differentiated categorically from fraud, because the distinction between "fraud" and

"abuse" depends on specific facts and circumstances, intent and prior knowledge, and available evidence, among other factors.

Promise #29

Q: Whose responsibility is it to prevent, detect and correct fraud, waste and abuse?

A. Associates, including executives and directors
B. Contractors and subcontractors (and their employees)
C. The Board of Directors
D. The Medicare Compliance Officer (For Medicare Business)

The correct answers are "A, B, C, and D". That's right. We are all responsible for preventing, detecting and correcting fraud, waste and abuse.

Promise #30

Q: I want to make sure I know the differences between fraud, waste and abuse. Help me match the examples to the correct definitions.

Examples are:

- A physician bills for services they know they did not perform.
- A physician orders excessive lab tests.
- A pharmacy bills for a brand name drug when a generic was dispensed.

Definitions are:

- Fraud: Intentionally submitting false information for money or another benefit
- Waste: Overusing or carelessly using health care services
- Abuse: Any action that may result in improper payment, unnecessary costs or items and services being provided that aren't medically necessary

The correct matches are:

A physician bills for services they know they did not perform is an example of Fraud.

A physician orders excessive lab tests is an example of Waste.

A pharmacy bills for a brand name drug when a generic was dispensed is an example of Abuse.

That's right. And remember, fraud involves intent and knowledge that what you're doing is wrong. Waste and abuse do not.

Preventing Fraud, Waste and Abuse

So how can you help prevent fraud, waste and abuse?

You can be aware of policies and rules:

- Read your department's and company's policies and procedures.
- Follow laws and regulations.
- Review guides and manuals.

You can make sure information is accurate:

- Check billing data.
- Verify information you receive.
- Do regular auditing.
- Monitor claims.

You can connect with others:

- Coordinate with other payers as needed.
- Ask about potential compliance issues in exit interviews.
- Communicate often with your colleagues.

Keep on the lookout for suspicious activity. And remember, when you see what you believe to be fraud, waste or abuse, report it.

Promise #31

Q: I want to help stop fraud, waste and abuse. What can I do?

A. Verify information you receive.
B. Make sure you understand and follow laws, regulations, policies and procedures.
C. Throw away all unnecessary paperwork related to claims.
D. Be on the lookout for suspicious activity – and report it.

The correct answers are "A, B and D". That's right. These are all ways you can help

us prevent fraud, waste and abuse.

Federal Laws and Regulations

You also need to be aware of federal laws and regulations that affect Medicare and federal health care programs:

- The False Claims Act prohibits someone from submitting false information to get payment or approval. For example, a provider isn't allowed to create a fake record or statement so they can submit a claim.
- The Anti-Kickback Statute prohibits someone from intentionally exchanging (or offering to exchange), anything of value, in an effort to induce (or reward) the referral of federal health care program business. For example, a hospital can't give money or another type of reward for referrals.
- The Stark Statute prohibits doctors from making certain referrals to an entity where they have a financial interest. For example, if a doctor owns or has an investment interest at an outpatient surgery center, they can't make referrals to that center for certain health services.
- HIPAA establishes safeguards to prevent access to Protected Health Information such as member data.
- Exclusions prevent payment to anyone who is excluded from participating in federal health care programs.

Promise #32

Q: I want to make sure I understand the federal laws and regulations. How does the name match up with the description?

The names are:

A. False Claims Act
B. Anti-Kickback Statute
C. Stark Statute
D. HIPAA
E. Exclusions

The descriptions are:

1. Prohibits doctors from making certain referrals to an entity where they have

a financial interest
2. Prohibits someone from submitting false information to get payment or approval
3. Establishes safeguards to prevent access to Protected Health Information
4. Prohibits someone from intentionally exchanging (or offering to exchange), anything of value, in an effort to induce (or reward) the referral of federal health care program business
5. Prevents payment to anyone who is excluded from participating in federal health care programs

The correct matches are:

> The False Claims Act prohibits someone from submitting false information to get payment or approval
>
> The Anti-Kickback Statute prohibits someone from intentionally exchanging (or offering to exchange), anything of value, in an effort to induce (or reward) the referral of federal health care program business
>
> The Stark Statute prohibits doctors from making certain referrals to an entity where they have a financial interest
>
> HIPPA establishes safeguards to prevent access to Protected Health Information
>
> Exclusions prevent payment to anyone who is excluded from participating in federal health care programs

Good job. You know the federal laws and regulations.

Consequences

Any person, group or plan faces serious consequences for committing fraud, waste or abuse. Some of the sanctions and penalties include:

- Being excluded from participation in federal health care programs (as a health plan associate, provider, supplier, etc.)
    - Addition to the Office of Inspector General (OIG) List of Excluded Individuals/Entities (LEIE)
    - Debarment from the Federal Employees Health Benefits (FEHB) Program

- License suspension or revocation
- Suspension of provider payments
- Loss of the of the right to sell Medicare plans
- Civil and criminal penalties, including arrest
- Fines ranging from $5,000 to over $100,000 — depending on the severity — for each false claim

If your behavior is noncompliant or fraudulent, it may also result in mandatory retraining or disciplinary action. Serious, repeated, intentional behaviors, or failure to report a possible violation of company policy may result in termination. In addition, failure to complete this course, which includes required fraud, waste and abuse training, may result in disciplinary action.

Promise #33

Q: If someone commits fraud, waste or abuse, what could

happen?

A. Sanctions
B. Loss of state property tax abatements
C. Exclusion from participation in federal health care programs
D. Criminal arrest
E. Loss of the right to sell Medicare plans

The correct answers are “A, C, D and E”. That’s right. Any person, group or plan faces serious consequences for committing fraud, waste or abuse.

Business Continuity

Many things can disrupt our business, like bad weather, system failures, or a security threat. In order to conduct business fairly, and ensure our members have access to care, we must be prepared to respond and recover from unexpected events.

For Medicare Business, we are required to develop, implement and maintain Business Continuity Plans (BCP). Each BCP has a plan owner, alternate plan owner, and a recovery team.

Be prepared. Speak with your manager about how you should respond and recover from disruptive events.

The BCP objectives are to:

- Make sure members have access to the care they need
- Protect the safety and well-being of associates, contractors, and visitors
- Restore critical operations
- Protect critical information
- Provide timely communications
- Resume normal operations as quickly as possible

Plan owners are responsible for:

- Leading response and recovery efforts
- Planning and implementing recovery operations
- Testing the plan each year

Plan owners are responsible for ensuring that staff are trained on their BCP.

Alternate plan owners assist plan owners in managing the response and recovery owners.

Recovery teams are responsible for:

- Implementing recovery operations
- Calling team members
- Assisting and organizing recovery
- Meeting response, recovery and restoration objectives

Have Concerns?

If you see something, say something. You are required to report all actual or suspected noncompliance or potential fraud, waste or abuse. All reported issues remain confidential to the greatest extent possible. And our non-retaliation policies protect anyone who makes a report in good faith. When you report concerns, we'll investigate and develop a plan of action to correct any issues we identify.

Keep reading to find out how to make a report.

You can contact your manager, your Compliance Officer or Aetna's Arizona Market Compliance Officer (delegted); or if you wish to remain anonymous, make your report via Aetna's (delegated) AlertLine ®.

Contact Aetna Investigative Services:

- Email Aetna Investigative Services: InvestigativeServices@aetna.com. Your email address is visible, so this is not anonymous.

And remember, you can always find ways to report in the Code of Conduct.

SIU

Our Company utilizes the Aetna Special Investigations Unit (SIU) to investigate suspected health care fraud, waste and abuse. This area also report instances of suspected fraud to the appropriate federal and state agencies, including NBI MEDIC, OPM-OIG, and State Departments of Insurance. For example, California requires us to report suspected fraud to the CDI Fraud Division within 60 days of reasonable belief (CIC §1872.4). Many other states have similar reporting requirements.

To learn more about SIU, contact your Compliance Officer.

Procurement

Suppliers help us deliver products and services – they're an extension of our company. But there can be risks. So when you work with a supplier, we have established a procurement process, supported by Aetna's Procurement Team.

From negotiating to signing a contract — it's important that you collaborate with the JV COE liaison to the Aetna Procurement team who provides advice to our company. They will help you follow laws and regulations, manage risks and get the most competitive pricing.

You can keep your promise to do business fairly when you work with suppliers ethically. Let's see how Procurement can help you.

Contacting Procurement

Procurement helps you with every step in the supplier engagement process: requests for proposals, pricing, competitive bidding, negotiations, supplier selection and contracting.

It is recommended that you contact the JV COE procurement liaison, which will connect with Procurement first — before you even get a quote, when practical.

Once you contact the JV COE procurement liaison and they contact Procurement, they will:

- Collaborate and Lead negotiations with the potential supplier
- Make sure we communicate appropriately with prospective suppliers
- Coordinate with our legal, privacy, security, information technology, compliance and risk management experts
- Manage the contract drafting process
- Ensure suppliers are property vetted (e.g., make sure a supplier is not listed on a federal exclusion list)
- Sign approved agreements, when appropriate (larger contracts that extend beyond Banner|Aetna)

Minimizing Risks

When you work with a supplier, here's how you can minimize risks:

- Report any potential conflicts of interest to Procurement, your manager or the Compliance Officer.
- Protect the company's confidential information.
- Protect the supplier's confidential information.
- Promote a positive supplier relationship – be professional and fair. For example, don't tell a supplier about another company's prices or quotes. And never accept bribes, gifts or kickbacks from a supplier, or use our name to endorse a particular supplier.

The bottom line is — always contact the JV procurement liaison and ask that they engage Procurement first. Procurement can efficiently and effectively help you handle suppliers fairly and get the most competitive pricing.

Promise #34

Q: We'd like to do some market research before we get started on this new campaign. I want to recommend my friend's marketing firm – they'd be great. Should I tell Procurement that my friend owns the company, or keep that to myself?

A. Tell Procurement about the company and that your friend owns it.
B. Tell Procurement about the company. You don't need to mention your friendship with the owner.
C. You can't recommend the company since your friend owns it.

The correct answer is "A". That's right. Procurement will ensure a fair and objective selection process.

Have Concerns?

Remember that you need to report any potential conflicts of interest with a supplier to your manager or to Aetna' s Arizona Market Compliance Officer (delegted) or your Compliance Officer.

We strictly forbid intimidation or retaliation against anyone who, in good faith, makes a compliant or reports a compliance violation.

Our Promises to the Community

Our promises to the community

Community

You are a part of our mission to build a healthy society. It's our promise to the community. We act on this promise through community involvement, support of diversity, and public policy leadership. Our environmental practices support a healthy environment because we know this supports a healthy society.

You can help keep our promise to the community. Treat customers, colleagues, business partners and members fairly. And when you treat others with respect, you build trust within the company and community.

Together, we can create a healthy environment inside and outside the company.

Conclusion

Congratulations!

Congratulations! You've finished the course. Your commitment to demonstrating the behaviors of The Banner|Aetn Way is the foundation of keeping the promises we make, which is the key to our success. If you have any questions about

compliance or ethics, you can contact:

- Your manager
- Your Compliance Officer
- Aetna’ s Arizona Market Compliance Officer (delegted)

Please sign the attestation and submit to your compliance officer and Aetna’s Arizona Market Compliance Officer (delegted).