

2021 Annual Compliance

1. 2018 Ascension Annual Compliance Course

1.1 AMITA Compliance Training



Notes:

Welcome to the AMITA Corporate Compliance course.

This course should take less than 30 minutes.

- You will navigate through the course by clicking the next button on each page.
- If you are unable to complete the course in one sitting, you can resume where you left off when you return to the course.

This course also includes an attestation that you have reviewed and agree to adhere to the Ascension Standards of Conduct. The attestation must be marked in order for the course to be completed.

1.2 Objectives



Objectives

By the end of this course, you will be able to:



- 01 Define Purpose**
Understand the purpose of the AMITA Compliance Program.
- 02 Understand Laws**
Have a general understanding of some of the laws that regulate healthcare.
- 03 How to Report**
Know how to report compliance issues and concerns.

Notes:

In this course, you will be able to:

- Understand the purpose of the AMITA Compliance program
- Have a general understanding of some of the laws that regulate healthcare, and
- Know how to report compliance issues and concerns

1.3 What is AMITA Compliance?



What is AMITA Compliance?

Remember, asking for help when something doesn't make sense or seem right is an important part of compliance.



Commitment	Ethical	Work-related	Knowledge
Our commitment to meeting legal and regulatory requirements.	Operating in accordance with ethical business practices.	Knowing the policies, procedure and laws that relate to your work.	Learning through training and education.

Notes:

AMITA's Corporate Compliance program is our commitment to meeting all legal and regulatory requirements and operating in accordance with ethical business practices.

How does this impact our daily work activities?

- The Compliance Program demonstrates our commitment to operating in accordance with all applicable laws and regulations that impact our areas of responsibility.
- We conduct business in accordance with ethical business practices including integrity, honesty, and accuracy.
- We know the AMITA policies, procedures and laws that relate to our work.
- We learn through training and education, and
- We ask for help when something doesn't make sense or seem right.

1.4 Why is Compliance Important?



Why is Compliance Important?

An effective compliance program will help AMITA:

- Follow complex laws, regulations, and standards
- Prevent violations from damaging our reputation in the community
- Identify concerns before they escalate
- Help minimize fines and penalties
- Contributes to efficient operation of our organization and is a key piece of our corporate culture



Notes:

There are a number of reasons why compliance is important.

- AMITA must follow numerous and complex laws, regulations, and standards.
- Violations can damage our reputation in the community.
- An effective compliance program can help identify potential concerns before they escalate and help minimize fines and penalties.
- Compliance contributes to the efficient operation of an organization and is a key piece of its corporate culture.

-

This important because, even well run organizations committed to following laws and regulations are still at risk for compliance violations.

1.5 AMITA Standards of Conduct

AMITA HEALTH

AMITA Standards of Conduct

Standards of Conduct describe the behavior expected of associates. The Standards of Conduct Booklet can be accessed in the Resources section of this course.

Relationship with Others
We interact with others in a sincere and authentic manner. We develop relationships with others based on honesty, fairness and mutual trust. We will not discriminate against individuals.

Compliance with Laws & Regulations
We operate in accordance with laws and regulations applicable to AMITA.

Human Resources
We strive to cultivate a work environment where associates are highly regarded.

Business and Ethical Practices
We are committed to ethical business conduct and integrity consistent with our Catholic tradition.

Conflicts of Interest
We act in a manner that is in the best interest of AMITA.

Confidentiality
We maintain the confidentiality of all organization information.

Notes:

AMITA carries out its healthcare ministry consistent with the AMITA Mission, Vision and Values. Integrity is one of AMITA's Core Values. The essence of integrity is a workplace in which we follow ethical and legal business practices.

The Standards of Conduct support the AMITA Core Values and are an integral part of the AMITA Compliance Program.

Standards of Conduct, which are listed on the screen, are intended to help you respond to questions and situations you may encounter in your daily work. The Standards of Conduct describe the behavior that is expected of associates as it relates to the following: Relationships with Others, Compliance with Laws and Regulations, Human Resources, Business and Ethical Practices, Conflicts of Interest, and Confidentiality.

Please take a moment to review the description of each area on the screen.

For more information on the Standards of Conduct, click on the purple button to view the AMITA Compliance Brochure.

2. Information Privacy and Security


2.1 Information Privacy and Security



Notes:

Let's consider some high-risk issues from a regulatory perspective. The next section of this training will cover Information Privacy and Security.

2.2 Information Privacy and Security




Information Privacy and Security

Data is a key component of AMITA operations:

- Received from external sources such as patients.
- Generated internally through many operational processes.
- Shared externally with entities such as clinical registries.

Privacy and Security compliance requirements include the Health Insurance Portability and Accountability Act (HIPAA), which covers patients' protected health information.



Notes:

AMITA has a moral and statutory obligation to safeguard its associates' and patients' information. As technology makes information sharing easier, fulfilling this obligation becomes more difficult.

Data is a key component of AMITA operations:

Data can be Received from external sources such as patients.

- Generated internally through many operational processes.
- Shared externally with entities such as clinical registries.

Privacy and Security compliance requirements include the Health Insurance Portability and Accountability Act (HIPAA), which covers patients' protected health information.

The following slides provide additional information and tips to help you avoid problems related to information privacy and security.

2.3 HIPAA: Two Main Sections



HIPAA: Two Main Sections



Privacy Rule
The Privacy Rule grants rights to individuals with regard to their health information and imposes obligations on covered entities for the uses and disclosures of protected health information (PHI).

Security Rule
The Security Rule requires organizations to safeguard electronic PHI (ePHI).

Notes:


The Health Insurance Portability and Accountability Act also known as HIPAA has two main sections:

The Privacy Rule and the Security Rule.


The Privacy Rule grants rights to individuals with regard to their health information and imposes obligations on covered entities for the uses and disclosures of protected health information (PHI).

The Security Rule requires organizations to safeguard electronic PHI (ePHI).

2.4 HIPAA: Additional Information



HIPAA: Additional Information



Health Insurance Portability and Accountability Act

Penalties
HIPAA imposes penalties on organizations and individuals who fail to keep PHI confidential in accordance with the law.


Health Information Technology for Economic and Clinical Health Act
HIPAA was updated to include the Health Information Technology for Economic and Clinical Health Act (HITECH), which among other things, requires healthcare organizations to notify the government and the individual of any "breach" of their PHI.

Notes:

HIPAA imposes penalties on organizations and individuals who fail to keep PHI confidential in accordance with the law.


HIPAA was updated to include the Health Information Technology for Economic and Clinical Health Act (HITECH), which among other things, requires healthcare organizations to notify the government and the individual of any "breach" of their PHI.

2.5 Protected Health Information (PHI)



Protected Health Information (PHI)

PHI includes information that can identify a person and that relates to their health condition, healthcare or payment for healthcare.



Examples of PHI:

- Name
- Address
- Zip Code
- Social Security Number
- Date of Birth
- Identifying Photo
- Patient Account Number
- Medical Record Number
- Diagnosis
- Email Address
- Telephone Number

Notes:

Protected Health Information, commonly referred to as PHI, needs to be carefully safeguarded in compliance with HIPAA regulations. Examples of PHI are:

Name

Address

Zip Code

Social Security Number

Date of Birth

Identifying Photo

Patient Account Number

Medical Record Number


Diagnosis

Email Address







Telephone Number

It only takes an inappropriate disclosure of one of the PHI examples on the screen to constitute a breach.

2.6 PHI Includes Any Format



PHI Includes Any Format

 Spoken	 Paper	 Telephone
 Electronic	 Mail	 Fax

 PHI includes information in any format, including the ones listed above.

Notes:

PHI includes information in any format, including the following:

Spoken

paper

telephone

electronic

mail

fax

2.7 Uses and Disclosures of PHI



Uses and Disclosures of PHI



Hospitals and physician offices may use and disclose PHI only as permitted or required under law, unless there is patient authorization. Examples of permitted uses and disclosures include:

Uses	Disclosures
Consulting with another provider for the treatment purposes	Public health reporting
Reviewing nurses' notes for quality review	Claims submission to insurance companies for payment
Patient registration	Accreditation organizations (e.g. The Joint Commission)

Notes:


Hospitals and physician offices disclose PHI to external individuals and organizations for legitimate business reasons.

Examples of appropriate disclosures of PHI include a doctor's order for treatment, a nurse's notes for quality reviews, patient registration, public health reporting, submission of claims information for insurance purposes, and disclosures to accreditation organizations.

2.8 HIPAA Data Breach



HIPAA Data Breach



What is a HIPAA data breach?

A breach is an inappropriate access, use or disclosure of unsecured PHI.

Reporting

In some instances, the organization must report breaches of unsecured PHI to the affected individual(s), to the Department of Health and Human Services, and potentially the media (depending on the size of the breach).

Local Policy

Report all potential breaches, regardless of the number of patients involved, to your supervisor and Compliance Officer in accordance with local policy.


Notes:

A breach is an inappropriate access, use or disclosure of unsecured Protected Health Information.

In some instances, the organization must report breaches to the Office for Civil Rights of the Department of Health and Human Services (OCR) and notify the individuals affected. There are currently 378 breaches affecting 500 or more individuals that are under investigation by the Office for Civil Rights from all healthcare organizations throughout the United States.

You must report all breaches, regardless of the number of records involved, to your supervisor and Compliance Officer in accordance with your policy.

2.9 Physical Security of PHI



Physical Security of PHI

Physical documents containing unsecured PHI must either be filed in the correct record or placed in a secure, locked bin to be shredded.

Observe all facility security safeguards:

- All employees and contractors should display a security badge while on premises
- Question individuals without a security badge or who appear suspicious
- Accompany all visitors when in restricted areas
- Do not allow unauthorized persons to follow you into restricted locations

Electronic PHI must be safeguarded through technology such as passwords and encryption.

Notes:


The next several screens illustrate safeguards that associates should practice to ensure compliance with HIPAA Privacy and Security regulations.

You must Observe all facility security safeguards:


This includes ensuring that All employees and contractors should display a security badge while on premises

- Questioning individuals without a security badge or who appear suspicious
- Accompanying all visitors when in restricted areas, and
- not allowing unauthorized persons to follow you into restricted locations

2.10 Password Management



Password Management



- 01 Strong Password**
Create a “strong” password that is difficult to guess
- 02 No Personal Information**
Do not use personal information when creating your password
- 03 Don't Write It Down**
Do not write down or post your ID and password on or with your computer or mobile device
- 04 Never Share It**
Do not share your password with anyone, including AMITA Technology Partners (ATP)

Notes:

There are several key considerations in password management:

Create a “strong” password that is difficult to guess

Do not use personal information when creating your password

Do not write down or post your ID and password on or with your computer or mobile device

Do not share your password with anyone, including AMITA Technology Partners (ATP)

2.11 Workstation Use and Security



Workstation Use and Security

To maintain proper workstation use and security, be sure that:



- 01 Your use of company devices are for work-related tasks only
- 02 You do not download or install unauthorized software
- 03 Computer screens containing PHI are not viewable by the public
- 04 In areas vulnerable to theft, workstations are physically secured using appropriate procedures and devices
- 05 You log out or invoke a password protected screen saver when leaving devices unattended

Notes:

To maintain proper workstation use and security, be sure that:

Your use of company devices are for work-related tasks only

You do not download or install unauthorized software

Computer screens containing PHI are not viewable by the public

In areas vulnerable to theft, workstations are physically secured using appropriate procedures and devices

You log out or invoke a password protected screen saver when leaving devices unattended

2.12 Physical Security of Laptops & Mobile Devices



Physical Security of Laptops & Mobile Devices

 Secure at all times	 Attend at all times	 Transport with caution	 Report when missing
Physically secure your laptop or mobile device at all times, and use a cable lock where appropriate.	Do not leave your laptop or other mobile device such as a smartphone or tablet unattended.	Use caution when transporting your device. For example, store it out of sight and locked in a trunk when possible. Do not leave it in your car overnight, even if your car is locked.	Promptly report missing or stolen devices to the ATP Service Desk and your supervisor.

Notes:

The safety and **Physical Security of Laptops & Mobile Devices is very important.**

Physically secure your laptop or mobile device at all times, and use a cable lock where appropriate.

Do not leave your laptop or other mobile device such as a smart phone or tablet unattended.


Use caution when transporting your device.

For example, store it out of sight and locked in a trunk when possible.

Do not leave it in your car overnight, even if your car is locked.


Promptly report missing or stolen devices to the AIS Service Desk and your supervisor.


2.13 Emailing PHI





Emailing PHI


If you need to send an e-mail containing patient information or other confidential information outside of the AMITA network in order to do your job, you must:

 **Encrypt**
You can encrypt an email by simply adding **-phi-** or **-secure-** to the subject line of your email. Keep it factual, short and professional (see images below).



 **Use Minimum Necessary Info**
Send the minimum necessary information only to the people who need to receive that specific information. Consider speaking to individuals rather than replying on email.



 Whichever word you decide to use, you must have the dashes before and after the word, just as it appears in the example. The words are not case sensitive. Do not include a patient's name in the subject line.

Notes:

If you need to send an e-mail containing patient information or other confidential information outside of the AMITA network in order to do your job, you must take the following steps to encrypt the message. This secures the information and ensures that it is only viewable by the recipient.

You can encrypt an email by simply adding **-Phi-** or **-secure-** to the subject line of your email.

Please see the sample message on the screen for a depiction of the subject line. Whichever word you decide to use, you must have the dashes before and after the word, just as it appears in the example. The most common reason that external e-mail messages are not encrypted is because the sender inserts spaces between the dash symbol and the word phi or secure.

Use the following guidelines in sending e-mail messages:

- When emailing confidential or protected information, send the minimum necessary information only to the people who need to receive that specific information.
- Keep emails factual, short and professional.

- Limit the use of email communications when discussing confidential business. Consider speaking directly with the other individual rather than relying on email.

2.14 Phishing tips




Phishing Tips

Tips to avoid being "phished":

- Watch out for emails labeled "from an external email address"
- Generic greeting – if you don't see your name be suspicious
- AMITA Health would never send out emails with links to verify email addresses or reset passwords
- Look for misspellings or incorrect grammar
- Always hover your mouse pointer over links in emails to see if they match where the email says it links
- If it appears to come from a colleague but you aren't sure, call that person or ask in a separate email



 What should I do if I open a phishing email?
If you do click a link, open an attachment or provide personal information shut down your computer and contact the AMITA Health Service Desk immediately for further direction.

Notes:

If you need to send an e-mail containing patient information or other confidential information outside of the AMITA network in order to do your job, you must take the following steps to encrypt the message. This secures the information and ensures that it is only viewable by the recipient.

You can encrypt an email by simply adding -Phi- or -secure- to the subject line of your email.

Please see the sample message on the screen for a depiction of the subject line. Whichever word you decide to use, you must have the dashes before and after the word, just as it appears in the example. The most common reason that external e-mail messages are not encrypted is because the sender inserts spaces between the dash symbol and the word phi or secure.

Use the following guidelines in sending e-mail messages:

- When emailing confidential or protected information, send the minimum necessary information only to the people who need to receive that specific information.
- Keep emails factual, short and professional.
- Limit the use of email communications when discussing confidential business. Consider speaking directly with the other individual rather than relying on email.

2.15 Social Media Guidelines



Social Media Guidelines

- Confidential**
Confidential information should never be disclosed. Referring to a patient by a nickname, diagnosis, or condition is a breach of confidentiality.
- During Work**
Refrain from using Social Media while on work time, unless it is work-related and authorized by your supervisor.
- Visibility**
Assume that all Social Media communication is visible to everyone, everywhere, all the times.
- Co-Workers**
Do not make disparaging remarks about co-workers.
- Work Environment**
Do not make comments that could create an intimidating or hostile work environment (e.g. offensive comments about age, race, sex, sexual orientation, religion, gender, etc.).
- Replying**
Do not respond to patient complaints or comments online.

Notes:

Consider the following guidelines related to the use of social media:

Confidential information should never be disclosed. Referring to a patient by a nickname, diagnosis, or condition is a breach of confidentiality.

Refrain from using Social Media while on work time, unless it is work-related and authorized by your supervisor.

Assume that all Social Media communication is visible to everyone, everywhere, all


the times.

Do not make disparaging remarks about co-workers.

Do not make comments that could create an intimidating or hostile work environment (e.g. offensive comments about age, race, sex, sexual orientation, religion, gender, etc.).

Do not respond to patient complaints or comments online.

2.16 Key Learning Points



Key Learning Points

Please avoid the following behaviors:

- Accessing information that you do not need to know in order to do your job.
- Misusing, disclosing or altering confidential information without proper authorization.
- Disclosing your sign-on and/or password to another person
- Using another person's sign-on and/or password.
- Leaving a secured application unattended.
- Allowing an unauthorized person to handle or have access to files that contain PHI or confidential information.
- Accessing PHI of friends, family, co-workers, VIPs, etc.

You may be subject to corrective action up to and including termination if you engage in these behaviors.

Notes:

Let's review a summary of what we have learned regarding information privacy and security.

Please avoid the following behaviors:

Accessing information that you do not need to know in order to do your job.

Misusing, disclosing or altering confidential information without proper authorization.

Disclosing your sign-on and/or password to another person

Using another person's sign-on and/or password.

Leaving a secured application unattended.

Allowing an unauthorized person to handle or have access to files that contain PHI or confidential information.

Accessing PHI of friends, family, co-workers, VIPs, etc.

3. High Risk Healthcare Regulations


3.1 High Risk Healthcare Regulations



Notes:

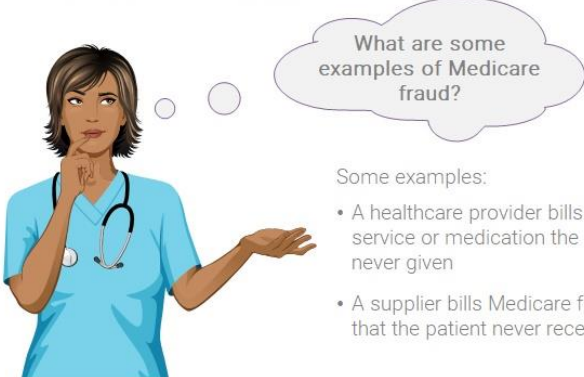
The next section of this course covers other important healthcare rules and regulations, the Federal False Claims Act, Stark Regulations and the Anti-Kickback Statute.

3.2 What is Medicare Fraud?



What is Medicare Fraud?

It is fraud when the Medicare program is **intentionally** billed for services or supplies the patient never received. Medicare loses billions of dollars to fraudulent claims every year.



What are some examples of Medicare fraud?

Some examples:

- A healthcare provider bills Medicare for a service or medication the patient was never given
- A supplier bills Medicare for equipment that the patient never received

Notes:

As recipients of federal health care program funds, including Medicare and Medicaid, AMITA is required by law to provide associates and contractors with information about the federal False Claims Act and state laws intended to prevent and detect fraud, waste and abuse in federal health care programs.


It is fraud when the Medicare program is **intentionally** billed for services or supplies the patient never received. Medicare loses billions of dollars to fraudulent claims every year.

Here are some examples of Medicare fraud:

- A healthcare provider bills Medicare for a service or medication the patient was never given

- .A supplier bills Medicare for equipment that the patient never received


3.3 What is Medicare Abuse?



What is Medicare Abuse?

Abuse describes practices that result in unnecessary costs to the Medicare program and are not consistent with the goals of providing patients with services that are medically necessary, meet professionally recognized standards, and are priced fairly.

Abuse can result in **waste** of healthcare resources.



Some examples:

- Billing for services that are not medically necessary.
- Charging excessively for services or supplies.
- Repetitive billing of incorrect or improper claims.

Notes:

Abuse describes practices that result in unnecessary costs to the Medicare program and are not consistent with the goals of providing patients with services that are medically necessary, meet professionally recognized standards, and are priced fairly.

Abuse can result in **waste** of healthcare resources.

Some examples of Medicare Abuse are:

Billing for services that are not medically necessary.

Charging excessively for services or supplies.
Repetitive billing of incorrect or improper claims.

3.4 Healthcare Fraud, Waste and Abuse




Notes:

Efforts to prevent, detect and report fraud, waste and abuse through a compliance program are extremely important in reducing federal healthcare expenditures.


In Fiscal Year 2016, the Medicare improper payment rate was 11 percent, representing **\$41 billion**.

In other words, during one year, the government paid an extra \$41 billion in healthcare costs that it should not have paid.


3.5 The False Claims Act




The False Claims Act



Claims Paid By:
The False Claims Act covers fraudulent claims paid by a government program such as Medicare or Medicaid.



Bill for Services
Submitting a claim for payment that contains false or fraudulent information could trigger the False Claims Act, so you should only bill for those services that are actually provided and documented in the medical record.



Compliance Booklet
Refer to the AMITA Standards of Conduct Booklet for additional information on the Federal and State False Claim Acts (Link available in Resource link in upper right-hand corner).

Notes:

The False Claims Act is a federal law that makes it a crime for any person or organization to knowingly make a false record or file a false claim with the government for payment.

The False Claims Act covers fraudulent claims paid by a government program such as Medicare or Medicaid.

Submitting a claim for payment that contains false or fraudulent information could trigger the False Claims Act, so you should only bill for those services that are actually provided and documented in the medical record.

Refer to the AMITA Standards of Conduct Booklet for additional information on the Federal and State False Claim Acts (Link available in Resource link in upper right-hand corner).

3.6 Protections under the False Claims Act

AMITA HEALTH

Protections under the False Claims Act

Associates are protected from being fired, demoted, threatened or harassed by their employer for filing a False Claims Act lawsuit with the government or providing information in good faith.

An illustration of a female healthcare professional with a stethoscope around her neck, wearing light blue scrubs. She is pointing her right hand towards a grey icon of a person standing next to a shield. The background features a green horizontal bar.

Notes:

The federal False Claims Act protects associates from being fired, demoted, threatened or harassed by their employer for filing a False Claims Act lawsuit with the government or providing information in good faith.

3.7 Anti-Kickback Statute and Stark Law

AMITA HEALTH

Anti-Kickback Statute and Stark Law


In addition to the False Claims Act, other federal laws and regulations have been passed to help prevent fraud and abuse, including the Anti-Kickback Statute and the Stark Law.

Anti-Kickback Statute
Prohibits giving or receiving anything of value in exchange for or to induce patient referrals for services or items payable by Medicare or Medicaid, unless an exception (known as a "Safe Harbor") is met.
Stark Law
Prohibits physicians from making referrals for specific types of services (called "designated health services") to entities with which the physician or his/her immediate family has a financial relationship, such as an ownership or compensation arrangement, unless an exception is met.
Also prohibits the entity from submitting claims for prohibited referrals of designated health services.

Notes:


(Information on slide)

3.8 Anti-Kickback Statute



Anti-Kickback Statute

- The Anti-Kickback Statute is an *intent-based* federal statute that applies to physicians, facilities and others who are in a position to make or influence referrals and covers activities such as:



```
graph LR; A[Discounts/Rebates] --> B[Kickbacks]; B --> C[Bribes]
```

- Potential violations of the Anti-Kickback Statute may include:
 - Paying more than fair market value for a physician's professional services in exchange for referrals
 - Reimbursing the cost of a physician's travel and expenses for a conference in exchange for referrals
 - Use of free or significantly discounted office space or equipment in exchange for referrals

Notes:

(Information on slide)

3.9 Stark Law



Stark Law

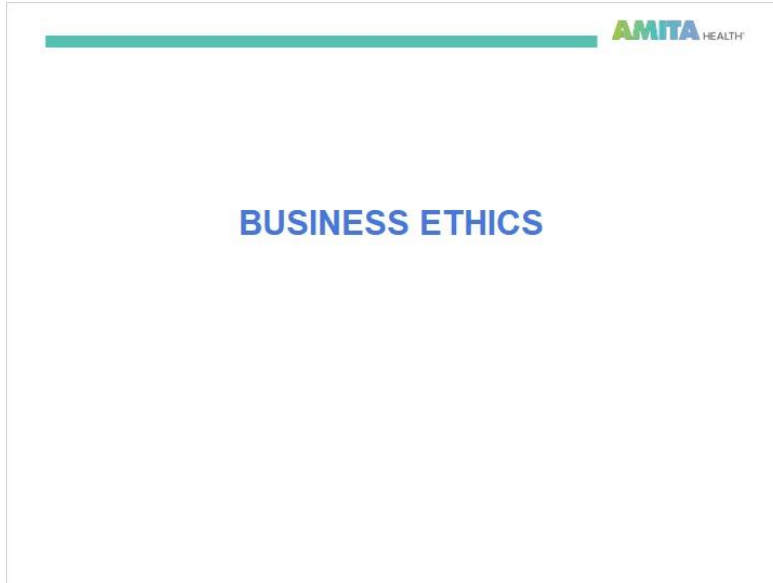
- The Stark Law prohibits physicians from making referrals for designated health services to an entity in which the physician or his/her immediate family member(s) has a financial relationship, unless an exception is met.
- If a physician profits from sending patients to a facility, it may affect his/her decision about what medical care the patient needs and where the patient receives the care.
- The Stark Law is a *strict liability* statute; intent is irrelevant.
- Potential violations of the Stark Law may include:
 - Lack of a current, written agreement for services provided by physicians (e.g., Medical Director agreements).
 - Paying a physician under an arrangement based on the volume of referrals the physician sends to the entity.
 - Lack of a current, written agreement for office space leased by physicians.

Notes:

(Information on slide)

4. Business Ethics


4.1 Business Ethics



Notes:


The next section addresses business ethics issues related to confidentiality and conflicts of interest.

4.2 Confidentiality



Confidentiality

In order to protect the confidentiality of AMITA data, we must:



- Not disclose confidential information to any outside unauthorized person or organization, or use such information for your personal benefit.
- Share confidential information about AMITA with associates only when they have a legitimate need to know the information in order to perform their job.
- Maintain confidential and proprietary information in a confidential, secure manner. Do not leave confidential information on desks, the copy machine, printer, or any other public areas.
- Sharing of confidential information extends beyond your employment at AMITA.

Notes:

Associates may be privy to confidential and proprietary information from internal sources as well as external organizations with whom we conduct business.

We need to treat all conversations - private, internal, email and even verbal - as potential external communication.

We must conduct ourselves as though everyone we talk with - in person or by phone, in a public space, text message or email - has the ability to share our conversation broadly.

This includes anyone and everyone we interact with - at a conference, in a meeting, in the lobby of a hotel or office building, in the restroom and even in a social setting.

In order to protect the confidentiality of AMITA data:

We should always Maintain confidential and proprietary information in a confidential, secure manner. Do not leave confidential information on desks, the copy machine, printer, or any other public areas.

We must Not disclose confidential information to any outside unauthorized person or organization, or use such information for your personal benefit.


We must not Share confidential information about AMITA with associates only when they have a legitimate need to know the information in order to perform their job.

Sharing of confidential information extends beyond your employment at AMITA.

4.3 Conflicts of Interest



Conflicts of Interest

Promptly disclose any relationships that might represent a conflict of interest.	Maintain arms length relationships with AMITA vendors.	Do not accept employment or consulting arrangements outside of your employment or make personal investments if they interfere with your job or unduly influence the decisions you make on behalf of AMITA.
	Refrain from accepting gifts, gratuities or entertainment intended to influence your judgement or actions.	

Notes:



In order to ensure that we act in the best interest of AMITA and comply with IRS regulations related to non-profit organizations, be mindful of the following:

Promptly disclose any relationships that might represent a conflict of interest. Don't wait for the annual conflict of interest disclosure reporting process.

In order to avoid potential conflicts of interest, associates should maintain arms-length relationships with AMITA vendors. Refrain from accepting gifts, gratuities or entertainment intended to influence your judgment or actions concerning AMITA business.

Don't accept employment or consulting arrangements outside of your employment or make personal investments if they interfere with your job or unduly influence the decisions you make on behalf of AMITA.

4.4 Language Services

Language Services

Language and communication assistance services must be provided free of charge to patients or companions with:

- **Limited English Proficiency ("LEP")** - those who do not speak English as their primary language and have a limited ability to read, write, speak or understand English.
- **Communication Challenges**- those with a physical or mental impairment that in some way limits or impacts the individual's ability to communicate. Examples of barriers may include sight, deaf, hard of hearing or speech impairments.

Qualified Interpreters are available through **video, phone, and in-person**. AMITA Health hospitals have designated ADA Administrators who will be on duty 24 hours a day, 7 days a week. **The ADA Administrator is the House Director on duty.**

Notes:

In order to ensure that we act in the best interest of AMITA and comply with IRS regulations related to non-profit organizations, be mindful of the following:

Promptly disclose any relationships that might represent a conflict of interest. Don't wait for the annual conflict of interest disclosure reporting process.

In order to avoid potential conflicts of interest, associates should maintain arms-length relationships with AMITA vendors. Refrain from accepting gifts, gratuities or entertainment intended to influence your judgment or actions concerning AMITA business.

Don't accept employment or consulting arrangements outside of your employment or make personal investments if they interfere with your job or unduly influence the decisions you make on behalf of AMITA.

4.5 Duty To Report



Duty To Report

Click each icon.
Before you can move on, click on each icon to see the example.

Some examples include


If you are aware of violations of laws, regulations, policies or the Standards of Conduct, you are required to report your concerns.




Notes:

(Information on slide)

4.6 How to Report



How to Report



<p>Associates are encouraged to go to their supervisor or manager. Associates may go to a higher-level manager if necessary.</p>	<p>Contact Human Resources if the issue is HR related.</p>	<p>Contact your local Compliance Officer.</p> <p>The list of Regional Compliance Officers:</p>	<p>Contact the Compliance Hotline via phone or Internet. The toll free number is listed below and the website is listed in the "Resources" tab.</p>
		<p><i>Link available in "Resources" tab</i></p>	<p>1.855.477.8861 AMITAhealth.ethicspoint.com</p>


Notes:

No Standards of Conduct, policies or training will anticipate every question or substitute for each individual's sense of honesty and integrity.

Where can you go for help if you have a concern or issue?

- Associates are encouraged to go to their supervisor or manager if at all possible.
- Associates may go to a higher-level manager if necessary.
- The Corporate Compliance Officer can be contacted in the event of a compliance issue or concern.
- Human Resources should be contacted for HR related issues.
- AMITA also provides the Compliance Hotline which is available to all associates either through the telephone at 855.477.8861, or through the Internet at www.DOTAMITAHEALTHDOTETHICSPPOINTDOTCOM

4.7 AMITA Compliance Hotline



AMITA Compliance Hotline



The Compliance Hotline is available 24 hours a day, seven days a week.

Phone calls are answered by an outside company and are not recorded or traced.

The same information is taken whether reported by phone or through the Internet.

You do not need to provide your name.

The Compliance Officer investigates each report and takes corrective action as appropriate.



Notes:

The Compliance Hotline is available to all AMITA associates.

- The hotline is available 24 hours a day, seven days a week.
- Phone calls are answered by an outside company and are not recorded or traced.
- The same information is taken whether reported by phone or through the web.
- Reporters can remain anonymous.
- At the end of the report, the reporter selects an identification number which allows them to follow-up on their report.
- The Compliance Officer investigates each report and takes corrective action if appropriate.

4.8 Non-Retaliation Policy



Non-Retaliation Policy

An effective compliance program requires engaged associates who are encouraged to report suspected wrongdoing.

Federal and State laws provide protections for associates that report issues in good faith.	It is AMITA's policy to protect associates who come forward with information about compliance concerns and to ensure that concerns are investigated and addressed without retaliation against the reporting associate.
---	--


Notes:

An effective compliance program requires engaged associates who are encouraged to report suspected wrongdoing.

AMITA has a non-retaliation policy that provides that no action will be taken against an associate for reporting a suspected violation in good faith. As a matter of fact, Federal and State laws provide protections for associates that report issues in good faith. Good faith means that the associate is honest and truthful.

5. Case Studies

5.1 Case Studies




Case Studies

Following are case studies with situations you may encounter in your daily work activities.

Notes:

Let's describe some situations that you might encounter in your daily work and how you should respond.


5.2 Case Study #1



Case Study #1

You pride yourself on doing a great job. Jim Thompson, a patient of yours, is being discharged today. He is so happy and he really appreciated the excellent care you provided. Jim has a surprise for you.

He has a gift card in an envelope. He hands it to you before he leaves the room and you open the envelope. What should you do?



- Tell him you appreciate the thought but you cannot accept the gift card.
- Accept the gift card and share with him other ways he can contribute to the hospital as well.
- Keep it but let your supervisor know that it was a gift from a patient who was very happy with his care.

Notes:

That's correct. It is not acceptable for AMITA associates to accept cash or gift cards from a patient.

You may want to suggest that the patient make a donation to the Hospital Foundation, if they so desire.

Incorrect (Slide Layer)

AMITA HEALTH

Case Study #1


You pride yourself on doing a great job. Jim Thompson, a patient of yours, is being discharged today. He is so happy and he really appreciated the excellent care you provided.

INCORRECT

It is not acceptable for AMITA associates to accept cash or gift cards from a patient.

You may want to suggest that the patient make a donation to the Hospital Foundation, if they so desire.

Keep it but let your supervisor know that it was a gift from a patient who was very happy with his care.



Correct (Slide Layer)

AMITA HEALTH

Case Study #1

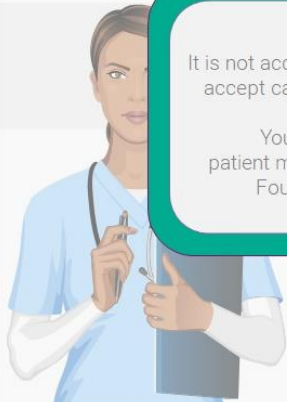
You pride yourself on doing a great job. Jim Thompson, a patient of yours, is being discharged today. He is so happy and he really appreciated the excellent care you provided.

CORRECT!

It is not acceptable for AMITA associates to accept cash or gift cards from a patient.

You may want to suggest that the patient make a donation to the Hospital Foundation, if they so desire.

Keep it but let your supervisor know that it was a gift from a patient who was very happy with his care.




5.3 Case Study #2

AMITA HEALTH

Case Study #2

My sister-in-law is a healthcare consultant.

Would it be a conflict if I recommended her to work on a project at my organization?



- Yes, you cannot make recommendations for family.
- Yes, you must direct to the application process and let them know you cannot help.
- No, as long as I disclose my relationship and do not benefit in any way.

Notes:

(Information on slide)

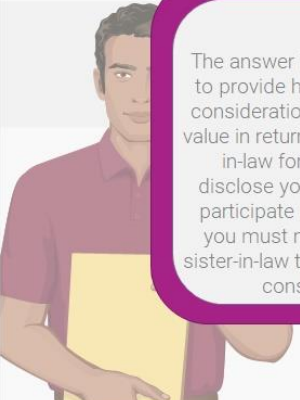
Incorrect (Slide Layer)

AMITA HEALTH

Case Study #2

My sister-in-law is a healthcare consultant.


Would it be a conflict if I recommended her to work on a project at my organization?



INCORRECT

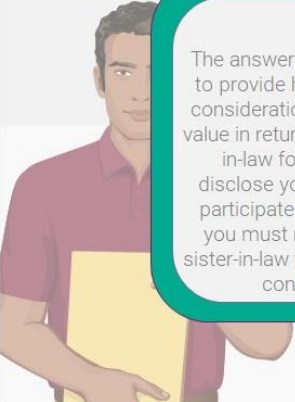
The answer is No. Unless you do something to provide her with an advantage of special consideration or if you receive something of value in return. If you recommend your sister-in-law for the project, you should fully disclose your relationship. You should not participate in the selection decision. Also, you must not share information with your sister-in-law that other prospective vendors or consultants would not have.

Correct (Slide Layer)



Case Study #2


My sister-in-law is a healthcare consultant.



CORRECT!

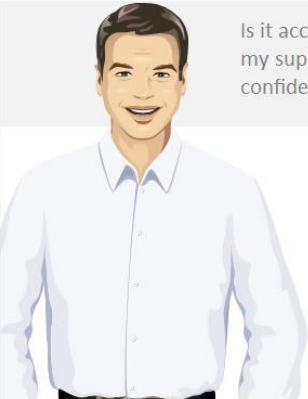
The answer is No. Unless you do something to provide her with an advantage of special consideration or if you receive something of value in return. If you recommend your sister-in-law for the project, you should fully disclose your relationship. You should not participate in the selection decision. Also, you must not share information with your sister-in-law that other prospective vendors or consultants would not have.

5.4 Case Study #3



Case Study #3

I worked for an AMITA vendor prior to my employment at AMITA. I have knowledge of the vendor's business strategies and operations that would be useful to AMITA.



Is it acceptable for me to share that information with my supervisor if he/she agrees to keep it confidential?


- No. Not only is it unacceptable, it can also be illegal.
- Yes, as long as they keep it confidential.
- Yes, especially if the vendor is going out of business anyway.

Notes:

I worked for an AMITA vendor prior to my employment at AMITA. I have knowledge of the vendor's business strategies and operations that would be useful to AMITA.

Is it acceptable for me to share that information with my supervisor if he OR she agrees to keep it confidential?

Incorrect (Slide Layer)



Case Study #3

I worked for an AMITA vendor prior to my employment at AMITA. I have knowledge of the vendor's business strategies and operations that would be useful to AMITA.


INCORRECT

The answer is No. Do not disclose confidential information learned through another job. It is unethical and possibly illegal to share confidential information you learn from your association with one employer with another employer should you leave the organization.

This prohibition on disclosing confidential information applies to associates who leave the employment of AMITA.

Information with
also be illegal.
il.
out of business

Correct (Slide Layer)



Case Study #3

I worked for an AMITA vendor prior to my employment at AMITA. I have knowledge of the vendor's business strategies and operations that would be useful to AMITA.


CORRECT!

The answer is No. Do not disclose confidential information learned through another job. It is unethical and possibly illegal to share confidential information you learn from your association with one employer with another employer should you leave the organization.

This prohibition on disclosing confidential information applies to associates who leave the employment of AMITA.

Information with
also be illegal.
il.
out of business


5.5 Case Study #4



Case Study #4

Occasionally, I share information about my job with friends and relatives on Facebook.

Since this is my personal Facebook account, is this acceptable?



- No, you can never post anything about your employment on Facebook.
- Yes as long as I don't post any information about patients.
- No, unless you get permission from HR to post to social media.

Notes:

(Information on slide)

Incorrect (Slide Layer)



Case Study #4

Occasionally, I share information about my job with friends and relatives on Facebook.

Since this is my personal Facebook account, is this acceptable?



INCORRECT

You are legally responsible for your opinions, comments or content on Facebook and other forms of digital social media. Never post any patient information on a social media site, including Facebook, YouTube, LinkedIn, Twitter, and other online social networks.

- No, unless you get permission from HR to post to social media.

Correct (Slide Layer)

AMITA HEALTH


Case Study #4

Occasionally, I share information about my job with friends and relatives on Facebook.

CORRECT!

You are legally responsible for your opinions, comments or content on Facebook and other forms of digital social media. Never post any patient information on a social media site, including Facebook, YouTube, LinkedIn, Twitter, and other online social networks.

No, unless you get permission from HR to post to social media.



5.6 Case Study #5

AMITA HEALTH

Case Study #5


Dr. Smith refers patients to our hospital. He said that he would refer more patients if we can provide him with discounted office space or staff to support his clinical practice.

Can we do this?

Yes, as long as the agreement is made in writing.

Yes, there is no legal requirement that prevents accepting more referrals of patients.

No, AMITA must charge the physician fair market value for any leased office space.



Notes:

(Information on slide)

Correct (Slide Layer)

AMITA HEALTH

Case Study #5

Dr. Smith refers patients to our hospital. He said that he would refer more patients if we can provide him with discounted office space or staff to support his clinical practice.

CORRECT!

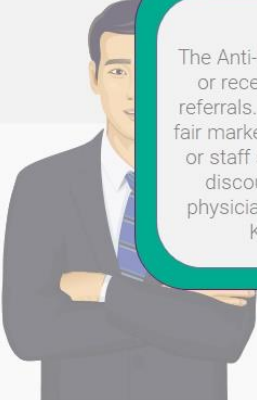
The Anti-Kickback Statute prohibits offering or receiving anything of value to induce referrals. AMITA must charge the physician fair market value for any leased office space or staff supporting his clinical practice, as discounted space or free services for physicians can lead to allegations of Anti-Kickback Statute violations.

AMITA must charge the physician fair market value for any leased office space.

AMITA can offer discounted office space or staff to support his clinical practice.

AMITA can offer discounted office space or staff to support his clinical practice, as long as it is in writing.

AMITA can offer discounted office space or staff to support his clinical practice, as long as it prevents accepting referrals from other providers.



Incorrect (Slide Layer)

AMITA HEALTH

Case Study #5

Dr. Smith refers patients to our hospital. He said that he would refer more patients if we can provide him with discounted office space or staff to support his clinical practice.

INCORRECT

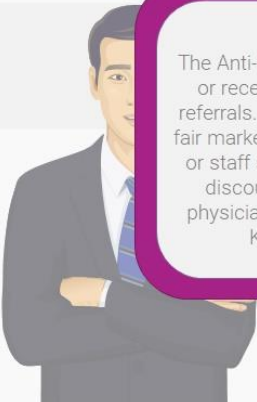
The Anti-Kickback Statute prohibits offering or receiving anything of value to induce referrals. AMITA must charge the physician fair market value for any leased office space or staff supporting his clinical practice, as discounted space or free services for physicians can lead to allegations of Anti-Kickback Statute violations.

AMITA must charge the physician fair market value for any leased office space.


AMITA can offer discounted office space or staff to support his clinical practice.

AMITA can offer discounted office space or staff to support his clinical practice, as long as it is in writing.

AMITA can offer discounted office space or staff to support his clinical practice, as long as it prevents accepting referrals from other providers.




5.7 Case Study #6



Case Study #6

I was working on discharging two patients around the same time, and I just realized that I gave Patient A the discharge instructions for Patient B.

What should I do?




- Tell both patients first thing.
- Contact my ministry's Compliance Officer.
- Let them know after you see your next patient.

Notes:

(Information on slide)

Incorrect (Slide Layer)



Case Study #6

I was working on discharging two patients around the same time, and I just realized that I gave Patient A the discharge instructions for Patient B.

INCORRECT

As soon as you realize the error has occurred, contact your Ministry's Compliance Officer and give as much detail as you can as to what occurred.

Please be prepared to discuss:

- What information was contained in the paperwork (name, DOB, SSN, diagnoses, medications, treatment plan, etc.)?
- Who was the information given to?
- Can the information be retrieved from patient A, or can confirmation be obtained that the information was destroyed?
- Contact information for the individual impacted (address and phone number).
- All these factors will help the Compliance team determine what level of risk the disclosure presents, and what type of notification may be required for the impacted individual.

Correct (Slide Layer)



Case Study

I was
rea

CORRECT


As soon as you realize the error has occurred, contact your Ministry's Compliance Officer and give as much detail as you can as to what occurred.

Please be prepared to discuss:

- What information was contained in the paperwork (name, DOB, SSN, diagnoses, medications, treatment plan, etc.)?
- Who was the information given to?
- Can the information be retrieved from patient A, or can confirmation be obtained that the information was destroyed?
- Contact information for the individual impacted (address and phone number).
- All these factors will help the Compliance team determine what level of risk the disclosure presents, and what type of notification may be required for the impacted individual.

just


5.8 Case Study #7



Case Study #7

One of my co-workers who is a coder told me that she always codes the Medicare "hospital acquired conditions" as being "present on admission" in order for the hospital to receive the higher payment.

What should I do?



- Share with coworker that this is illegal and putting the hospital at risk for fines and penalties.
- Say nothing to her and try to film her in the action, as evidence for your supervisor.
- Help her code correctly and say nothing to your supervisor or department director.

Notes:

(Information on slide)

Incorrect (Slide Layer)

AMITA HEALTH

Case Study #7

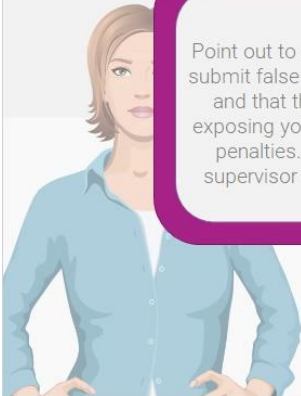
One of my co-workers who is a coder told me that she always codes the Medicare "hospital acquired conditions" as being "present on admission" in order for the hospital to receive additional reimbursement.

and putting the
in the action, as

INCORRECT

Point out to your co-worker that it is illegal to submit false claims to the Medicare program and that these coding practices may be exposing your hospital to potential fines and penalties. Please discuss this with your supervisor or department director as well.

Help her code correctly and say nothing to your supervisor or department director.



Correct (Slide Layer)

AMITA HEALTH

Case Study #7

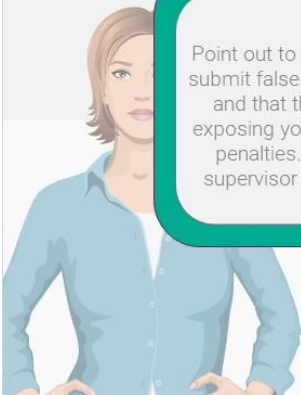
One of my co-workers who is a coder told me that she always codes the Medicare "hospital acquired conditions" as being "present on admission" in order for the hospital to receive additional reimbursement.

and putting the
in the action, as

CORRECT!

Point out to your co-worker that it is illegal to submit false claims to the Medicare program and that these coding practices may be exposing your hospital to potential fines and penalties. Please discuss this with your supervisor or department director as well.


Help her code correctly and say nothing to your supervisor or department director.



5.9 Case Study #8

AMITA HEALTH

Case Study #8



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

- No, as long as you reported the violation in good faith.
- Yes, it is very important that you have all the facts before you report a violation.
- Yes, it is not good stewardship of resources to investigate a violation that did not actually occur.

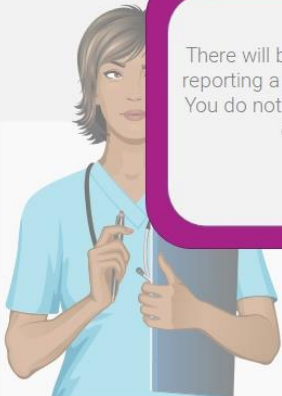
Notes:

(Information on slide)

Incorrect (Slide Layer)

AMITA HEALTH

Case Study #8



INCORRECT

There will be no action taken against you for reporting a suspected violation in good faith. You do not need to provide your name when calling the Values Line.


Standards

on in good faith.

all the facts before

- Yes, it is not good stewardship of resources to investigate a violation that did not actually occur.

Correct (Slide Layer)



Case Study #8

CORRECT!

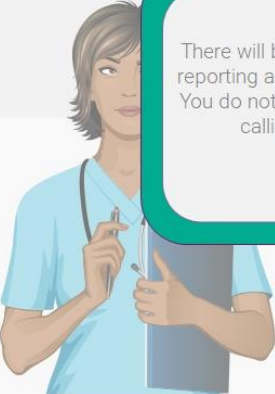
There will be no action taken against you for reporting a suspected violation in good faith. You do not need to provide your name when calling the Compliance Hotline.

Yes, it is not good stewardship of resources to investigate a violation that did not actually occur.

Standards


on in good faith.

all the facts before




6. Course Summary

6.1 Key Takeaways



Key Takeaways

- 01 Compliance is everyone's responsibility.
- 02 Everyone is expected to understand and comply with applicable laws, regulations and organizational policies.
- 03 Whether an activity presents potential compliance concerns often depends on specific facts and circumstances.
- 04 Failing to address identified concerns can increase risk to our organization.
- 05 The best defense is having an active and effective Compliance Program.



Notes:

Our commitment to Compliance begins and ends with each associate. Let's

review some key takeaways from the course.

(Information on slide)

6.2 Your Role as an Associate

YOUR ROLE	YOUR ROLE
As an associate	As a leader
<ul style="list-style-type: none">• Understand the laws and regulations that impact your area of responsibility.• Speak up when concerned about questionable behaviors.• Be alert for potential issues and ask for guidance.• Report potential Legal and Business Ethics violations to your Supervisor, Human Resources, the Compliance Officer or the Values Line.	<p>Demonstrate your commitment to regulatory compliance and business ethical standards.</p> <ul style="list-style-type: none">• Set the "tone at the top."• Business ethics are the responsibility of each individual associate and start with the leadership team.• Be accessible to your associates to report compliance/business ethics concerns.• Resolve associate complaints.

Notes:

Compliance is everyone's responsibility. As an associate, you are expected to:

- Understand the laws and regulations that impact your area of responsibility.
- Speak up when concerned about questionable behaviors.
- Be alert for potential issues and ask for guidance.
- Report potential Legal and Business Ethics violations to your Supervisor, Human Resources, the Compliance Officer or the Compliance Hotline

Leaders have a role in receiving and responding to questions and concerns raised by associates and others you lead. How you respond to these questions and concerns is key to others having the trust and confidence to bring important matters to your attention.

Leaders are expected to:

- Set the “tone at the top”.
- Business ethics are the responsibility of each individual associate and start with the leadership team.
- Be accessible to your associates to report compliance/business ethics concerns.
- Resolve associate complaints.

6.3 STANDARDS OF CONDUCT ATTESTATION

(Short Answer, 0 points, 1 attempt permitted)

 ASCENSION

STANDARDS OF CONDUCT ATTESTATION

All associates must complete this Standards of Conduct Attestation by **typing** their name and clicking submit.

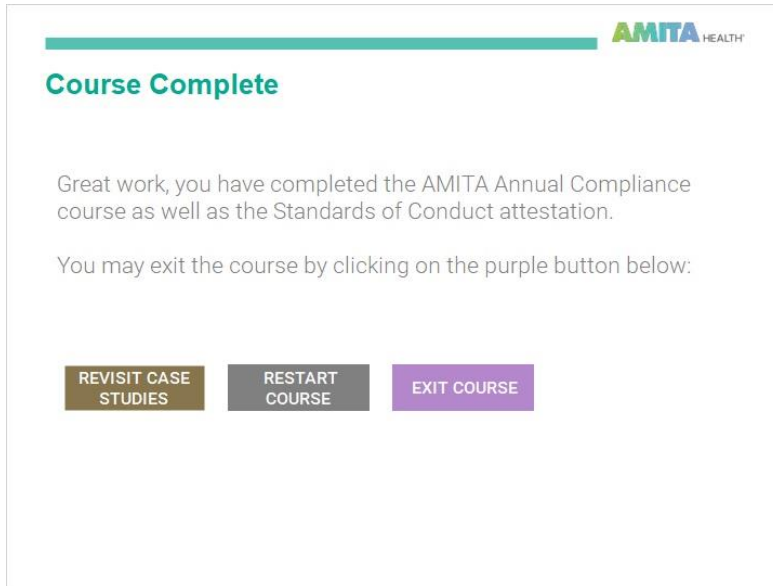
- ✓ I acknowledge that the Standards of Conduct have been explained to me and I agree to follow them.
- ✓ I understand that compliance with the Standards of Conduct is a condition of my continued employment or association with AMITA.
- ✓ I will uphold the highest standard of ethical and legal business practices. I will not tolerate illegal or questionable activity and promise to identify, report and prevent such activity.
- ✓ I am expected to maintain the privacy and security of all confidential information, including patient protected health information whether in paper or electronic format. I agree to adhere to AMITA policies, which includes maintaining the confidentiality of information in all electronic systems to which I have access.
- ✓ I will not use, disclose or discuss confidential and protected health information with others unless permitted to do so based on my job responsibilities or as required by law.

Notes:

This is an attestation form which must be completed by all associates.

Please type your name on the attestation statement in recognition of your commitment to abide by the Standards of Conduct.

6.4 Course Complete



AMITA HEALTH

Course Complete

Great work, you have completed the AMITA Annual Compliance course as well as the Standards of Conduct attestation.

You may exit the course by clicking on the purple button below:

REVISIT CASE STUDIES RESTART COURSE EXIT COURSE

Notes:

Great work, you have completed the AMITA Annual Compliance course as well as the Standards of Conduct attestation.

You may exit the course by clicking on the purple button below: