Compliance Education for Medical Staff Members



Developed by Providence Health & Services

February 2015

Welcome!

Welcome to the Integrity, Compliance, Privacy and Security education for medical staff members (and their staff).

This education will highlight key risks that your medical practice is facing, including obligations to follow federal and state laws and regulations and your own internal policies.

Objectives

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

- Identify and avoid behaviors associated with fraud, waste and abuse
- Understand how documentation affects the accuracy of claims
- Recognize privacy and security vulnerabilities in the workplace
- Identify key privacy and security responsibilities in the workplace and the penalties for violations

There are five review questions at the end of this module to test your knowledge and comprehension. This module should take you about 15 minutes to complete.

Quality of Care

As health care providers, we are committed to providing the best care and service at every patient encounter.

Fraud, Waste and Abuse

One of the serious risks facing health care providers is billing for services that were not provided and misrepresenting what services or products were provided. These are examples of fraud, waste and abuse or false claims.

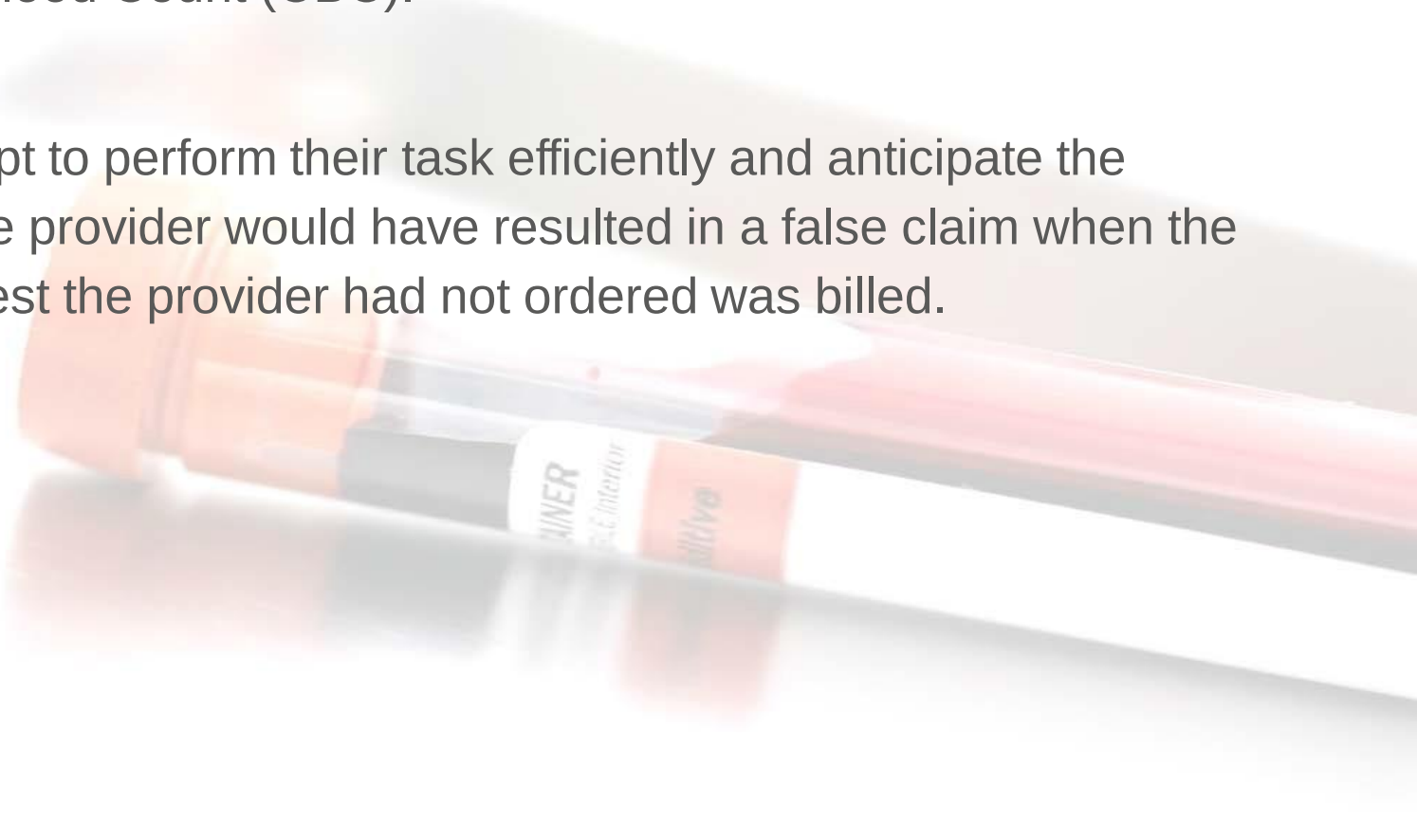
Penalties for these types of false claims could result in significant fines, jail time and or exclusion from participation in federal and state programs such as Medicare and Medicaid.

Click here to launch a video scenario on fraud, waste and abuse.

Accuracy and Clarity

Gloria and Juan intended to save Dr. Pang the extra step of ordering the Differential because it is often ordered with the Complete Blood Count (CBC).

Their attempt to perform their task efficiently and anticipate the needs of the provider would have resulted in a false claim when the additional test the provider had not ordered was billed.



Accuracy and Clarity, cont…

Even if your role is not related to patient care or billing, assumptions and miscommunication can lead to inefficiency and confusion. Whether you are the **giver** or **receiver** of information, **you should always strive to communicate clearly and accurately:**

Giving Information: Be concise, but be sure to provide **ALL** necessary information. Ask the receiver to repeat your request or statement to ensure mutual understanding. Answer clarifying questions. If appropriate, follow up with an email that documents the discussion or agreements.

Receiving Information: Listen carefully and ask clarifying questions. If the information or request is complex, take notes during the conversation or immediately after. Follow up with the giver later if additional questions arise and **never** make assumptions.

False Claims Act

The potential false claim shown in the video scenario is an example of fraud and abuse. The federal False Claims Act (31 USC 3729-33) 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.

This means that all claims for payment must contain true, complete, and accurate information. The accuracy of each claim submitted is dependent on the documentation provided, including diagnosis and written orders. Codes should be selected that most appropriately describe the services rendered to a patient. Other examples of false claims include:

- Billing for services that were not provided or not documented
- Billing for services that are not medically necessary
- Providing services at substandard quality where the government would not pay for the services

Penalties and Fines

A person who knows a false claim was filed for payment can file a lawsuit in Federal Court on behalf of the government and, in some cases, receive a reward for bringing original information about a violation to the government's attention.

Some states have a False Claims Act that allows a similar lawsuit in state court if a false claim is filed with the state for payment, such as under Medicaid or Workers' Compensation.

Penalties are severe for violating the federal False Claims Act and may include significant fines, jail time and/or exclusion from participation in federal and state programs such as Medicare and Medicaid. Financial penalties can be up to three times the value of the false claim, plus fines ranging from $5,500 to $11,000 per claim.

Next let’s take a look at Privacy and Security

Why do Privacy and Security matter?

Privacy is important in health care delivery. Without privacy in your medical practice, patient trust is diminished and without patient trust they are highly unlikely to share confidential information with you. Patients who trust their health information will be kept private and secure will be more willing to discuss their symptoms, conditions, and past and present risk behaviors.

Information Security describes the practices and technology used to protect this confidential information. Your practice must incorporate appropriate administrative, technical and physical safeguards to protect your patients' information.

Why do Privacy and Security matter, cont.

The Health Insurance Portability and Accountability Act (HIPAA) requires medical practitioners to protect patient health information and gives patients certain rights regarding their protected health information (PHI).

There are other federal and state laws that protect patient information. Ask your privacy officer or office manager if your office has additional privacy and security policies and procedures that you should follow.

Information that Requires Protection

Confidential information that requires protection includes:

Protected Health Information (PHI) is any information that can be used to identify an individual and that is created or received in the course of providing a health care service such as diagnosis, treatment, payment or health care operations. PHI can be in any form, including written, electronic, oral or video.

Personally Identifiable Information (PII) is information that can be used to uniquely identify an individual. It includes a person's name in combination with identifying information such as social security number, date of birth, credit or debit card number or driver's license number.

Many federal and state laws require that individuals and/or the government be notified if PHI or PII has been compromised.

Information that Requires Protection, cont.

Medical staff members must use good judgment when granting their employees and business partners access to PHI and PII, and should educate their workforce as appropriate on risk protection measures.

Likewise, medical staff members must be diligent in removing an employee's or business partner's access to PHI and PII upon termination of employment or contract.

Key Privacy Risks

The following privacy practices will help make sure protected health information (PHI) is handled properly:

- Only access information if you **have a need to know as part of your job**
- If you have a legitimate need to know, use or disclose only the **minimum information necessary** to do the job

Use or disclosure of PHI for purposes other than treatment, payment or health care operations generally requires **authorization** from the patient. Check with your privacy officer if you have questions.

Privacy Video Scenario

Click here to launch a video scenario on privacy.

Privacy Violations

Selena inappropriately accessed and disclosed her co-worker's PHI — a serious violation that could potentially result in fines and criminal charges.

You may **never** access medical records of your friends, relatives, other staff members or anyone else unless you need this information to perform your job duties. You may **never** share this information with anyone that does not have a need to know. You can be fined and face civil or criminal charges, including jail time, for inappropriate access or disclosure of patient privacy. In 2010, a researcher at UCLA School of Medicine was sentenced to four months in jail for inappropriately accessing patient records.

You should **never** share protected health information, confidential, proprietary work-related information, photographs or videos about the workplace on personal or social media sites (e.g., Facebook, Twitter or My Space). You can be held **personally** and **legally** responsible for online opinions and comments that you make public, even on personally maintained sites and web-pages.

Other Violations

What other privacy and information security violations did you spot in the video?

Multiple patient records seem to be **open** and **scattered** around Selena's desk.

There appears to be **personally identifiable information** (PII) in clear view on the chart behind Selena.

Selena has various **passwords** written on sticky notes on her monitor.

Selena leaves her desk without **locking** her keyboard or **securing** patient files.

Security Violations

Keeping **computers**, **network systems**, **laptops** and other **mobile devices** secure is essential to protect patient and workforce information.

Take care to use *different* passwords for your work network account and personal accounts to help protect you and your personal information. To be safe, choose unique passwords for other internet accounts, including financial, retail, social media, and others.

- Never share passwords with anyone
- Don’t include personal details in your password, such as your birth date, family or pet names, favorite sports teams, etc.
- Use at least eight characters
- Don’t use words found in a dictionary
- Use a mixture of uppercase and lowercase letters with numbers or characters. **Example:** rA74bbiT

Conclusion

As health practitioners and medical office workforce members, you should now have an understanding of:

- ✓ The importance of accurate billing and coding
- ✓ Why the accuracy of each claim submitted is dependent on the documentation provided
- ✓ When it is and is not appropriate to look at a person's medical record, and
- ✓ Security best practices

Question #1

1. **What constitutes a false claim *(Choose all that apply)***

a) Billing for services that were not provided or not documented
b) Billing for services that have documentation that supports the claim
c) Billing for services that are not medically necessary
d) Both a and c

Question #1 – Answer

1. **What constitutes a false claim *(Choose all that apply)***

a) Billing for services that were not provided or not documented
b) Billing for services that have documentation that supports the claim
c) Billing for services that are not medically necessary
d) Both a and c

The correct answer is d. You should never bill for services that were not provided, documented or medically necessary.

Question #2

2. Penalties for false claims can include

a) Jail time
b) Fines
c) Exclusion from participation in federal and state programs
d) All of the above

Question #2 – Answer

2. Penalties for false claims can include

a) Jail time

b) Fines

c) Exclusion from participation in federal and state programs

d) All of the above

The correct answer is d. Penalties for false claims could result in significant fines, jail time and/or exclusion from participation in federal and state programs such as Medicare and Medicaid.

Question #3

3. Effective passwords use a mixture of uppercase and lowercase letters with numbers or characters

a) True

b) False

Question #3 – Answer

3. Effective passwords use a mixture of uppercase and lowercase letters with numbers or characters

a) True

b) False

True. Effective passwords use a combination of uppercase and lowercase letters with numbers or characters.

Question #4

4. **I can post confidential information that I heard about at work on my Facebook page because it is my personal web-site**

a) True

b) False

Question #4 – Answer

4. I can post confidential information that I heard about at work on my Facebook page because it is my personal web-site

a) True

b) False

False. You may never post confidential information you have learned at work or post any patient protected health information without authorization from the patient. Even disclosing the fact that someone is a patient at your clinic requires the patient's authorization.

Question #5

5. Personally Identifiable Information is information such as someone's name plus one of the following:

a) Social Security Number
b) Driver's license or state identification card number
c) Account or credit or debit card number
d) All of the above

Question #5 – Answer

5. Personally Identifiable Information is information such as someone's name plus one of the following:

a) Social Security Number

b) Driver's license or state identification card number

c) Account or credit or debit card number

d) All of the above

Thank you!

Please contact your practice manager to document your completion of this compliance education module.