2018 1st Quarter
Volume 12, Issue 1

UB|MD PHYSICIANS' GROUP

Compliance Quarterly

From the Compliance Office...

1st Quarter Delay

We apologize for the delayed distribution of this 1st Quarter *Compliance Quarterly*. After reviewing our year-end numbers for overall completion of the 2017 3rd Quarter Mandatory Fraud, Waste & Abuse training, we found it necessary to take time to follow up with many practice plans in order to get their personnel to complete the training. Additionally, we had to follow up with a large number of faculty physicians regarding their completion of Conflict of Interest training that we were asked to distribute in mid-December. The process for both ended up being more time consuming than we had hoped.

Compliance Training Update

New Provider E/M & Documentation Training

This is a one session training class. All are welcome to attend any of the sessions. It's also a good refresher for the not-so-new providers! ***Please contact Bev if you would like to attend a session so that she can be sure to have enough materials for all attendees.***

Location & Time: 77 Goodell St., Room 310F, 11:30AM

2018 Dates: April 24
May 8 & 22
June 12 & 26
July 10 & 24
August 7 & 21
September 11 & 25
October 9 & 23
November 6 & 20
December 4 & 18

Lunch-n-Learn

Sessions are usually held once a month. Bring your lunch, and join us as we cover a variety of important topics related to coding and compliance! AAPC & AHIMA CEUs are often available for the sessions. All are welcome to attend. ***If you would like to be added to the session contact list, please contact Bev as noted to the right.***

Location & Time: 77 Goodell St., Room 205, 12:00-1:00PM

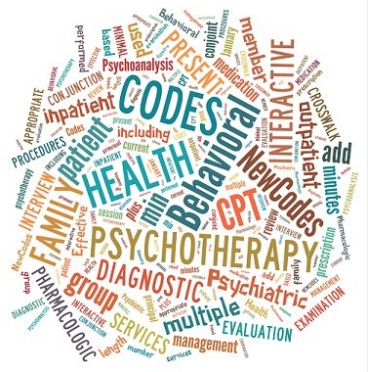
2018 Dates: 4/17, 5/15, 6/19, 8/15, 9/18, 10/16, 11/13 & 12/11
(no class in July)

Inside this issue

From the Compliance Office 1
Compliance Training Update...1
Why Do We Audit Records?.....2
Training Reminder.....3
Student Documentation 5
Compliance Culture 5
Cybersecurity: Phishing.....8

Training Questions:

If you have questions on any the training, please contact Bev Welshans by telephone (888-4702) or e-mail: welshans@buffalo.edu



Why Do We Audit Records?

By: Beverly Welshans, CHC, CPMA, CPC, COC, CPCI, CCSP
Director of Audit & Education

Quality health care is based on accurate and complete clinical documentation in the medical record. The best way to improve clinical documentation and the financial stability of our Practice Plans is through medical record audits. They are necessary to determine areas that require improvements and corrections. Investigations for inaccurate and inappropriate claim filing have increased in recent years. Federal agencies received additional funding and staffing to conduct investigations.

The Coding Corner

In 2000, the Office of Inspector General (OIG) published Compliance Program Guidance for Individual and Small Group Physician Practices. OIG strongly recommends periodic reviews of your billing practices to monitor your compliance with statutes and regulations associated with claims for reimbursement.

This FAQ addresses the following:

- Why should we consider auditing our medical records?
- What is the difference between a prospective audit and a retrospective audit?
- Who should be our auditor?
- How many charts should we audit?
- How do we select the sample of charts for review?
- What resources are required to perform an audit?
- What is the objective of a chart audit?
- What types of findings should we expect?
- What are examples of underbilling?
- What are examples of overbilling?
- How are the results best recorded and reported?
- What do we do after the audit is completed?

The Audit Program in the UBMD Compliance Plan has been modeled after this OIG Guidance. The goal of our audits is to provide providers with the education and guidance they need for more efficient documentation and to improve the financial stability through compliant health care records.

Medical record audits specifically target and evaluate procedural and diagnosis code selection as determined by physician documentation. Once areas of weakness are revealed through an audit, we can present the audit findings to the providers and identify opportunities for training to improve their compliance.

Continued on page 3

Continued from page 2

Our audits are intended to be educational rather than punitive and there are many reasons for performing them:

- To determine outliers before large third party payers find them in their claims software and initiate their own audit;
- To protect against fraudulent claims and billing activity;
- To help identify and correct problem areas before insurance or government payers challenge inappropriate coding;
- To help prevent governmental investigational auditors like recovery audit contractors (RACs) or zone program integrity contractors (ZPICs) from knocking at your door;
- To remedy undercoding, improper unbundling habits, and code overuse and to bill appropriately for documented procedures;
- To identify reimbursement deficiencies and opportunities for appropriate reimbursement;
- To stop the use of outdated or incorrect codes for procedures;
- To verify ICD-10-CM and HCC Coding compliance.

> ***"That which is measured improves. That which is measured and reported improves exponentially."***
>
> *~ Karl Pearson, Mathematician*

The audits are required on an annual basis with a minimum of 10 encounters per billing provider. Any provider with an initial audit compliance score less than 85% is provided with training on their deficiencies and subject to a second, more detailed, audit to monitor for improved compliance.

Our office is also available to conduct focused audits upon request if there is a concern raised for a certain procedure, provider, coder or other issue.

Compliance Training Reminder

According to the UBMD Compliance Plan, all UBMD personnel are required to complete a minimum of two (2) hours of compliance training biennially (every two years). This includes all providers and staff.

While the Compliance Plan lists several ways to earn credits and report it to the Compliance Office, the Compliance Office sends out four *Compliance Alliance* newsletter each year which contain articles, training schedules for Lunch-n-Learn sessions and for new providers, regulatory updates, recent news stories pertinent to the healthcare field, and other important information. Each newsletter includes a simple five question quiz at the end directly taken from the information in the newsletter. It takes only a short time to read and to complete the quiz online. Each of the four newsletter quizzes, when successfully completed, is a .25 hour credit of compliance training, so if you complete all four each year, it's a pretty convenient, non-time consuming, and convenient way to meet the biannual 2 hours of training requirement.

The 3rd quarter newsletter also currently serves as the annual mandatory Fraud, Waste & Abuse (FWA) training that is required annually by The Centers for Medicare and Medicaid Services (CMS) as well as many 3rd party payors. All UBMD employees must complete this particular newsletter & quiz.

In 2017 we noticed a drop-off in completed newsletter quizzes and FWA training quizzes, and found it necessary to follow-up, in some cases several times, with practice plans to have all employees complete it. Should we continue to have this problem, it may become necessary to look into other training methods, such as mandatory face-to-face training sessions. We hope to see better participation numbers in 2018.

As always, please contact us if you have any questions regarding required training.

CMS Allows Student Documentation of E/M Services!

By: Lawrence C. DiGiulio, Chief Compliance Officer

Effective March 05, 2018: CMS has released Change Request 10412 which revises Chapter 12, Section 100.1.1 of the Medicare Claims Processing Manual to allow the teaching physician to verify in the medical record any student documentation of components of E/M services, rather than re-documenting the work. This is an important change for teaching physicians and those who provide coding services to teaching physicians.

CR 10412 states the following specifics regarding this change:

- Students may document services in the medical record.
- The teaching physician must verify in the medical record all student documentation or findings, including history, physical exam and/or medical decision making.
- The teaching physician must personally perform (or re-perform) the physical exam and medical decision making activities of the E/M service being billed, but may verify any student documentation of them in the medical record, rather than re-documenting this work.

"This is an important change for teaching physicians and those who provide coding services to teaching physicians."

CMS notes that this change was identified by the Documentation Requirement Simplification workgroup and is part of a broader goal to reduce administrative burden on practitioners.

CAUTION: Though this is intended to reduce the documentation burden, it is important that care is taken to develop documentation standards so that there is no question that the teaching physician verified the student's documentation and personally performed the physical examination and medical decision-making of the E/M service.

To comply with this new rule change and ensure we can compliantly bill for these services, we have developed a Student E/M Documentation Attestation similar to the PATH Attestation with which you are all familiar. On March 5, 2018, this attestation can be found in Allscripts (in the Provider Attestation section of your Notes) and should be added to each student documented note. The attestation reads:

MEDICAL STUDENT E/M DOCUMENTATION ATTESTATION:

I have seen, personally examined and assessed the patient to establish a plan of care. I have reviewed the medical record and verify that all student documentation or findings, including history, physical exam and/or medical decision making are accurate. I have performed or re-performed, the physical exam and medical decision making activities to the extent they were conducted by a student.

This does not mean students may act as scribes and document their own actions for the same patient visit. A scribe cannot participate in care by preparing a history, conducting any part of the examination or asking the patient questions.

If you have any questions about this or any compliance matter, please contact me directly at (716) 888-4705 or the Compliance Hotline at (716) 888-4752.

General Compliance: A Compliance Culture

By: Sue Marasi, CHC, CPCA, Compliance Administrator

It seems we hear a lot about the importance of "culture" in many aspects lately, especially in sports. Healthcare and compliance are no different. Consider this Merriam-Webster definition of culture:

a: *the customary beliefs, social forms, and material traits of a racial, religious, or social group; the characteristic features of everyday existence (such as…a way of life) shared by people in a place or time;*

b: the set of shared attitudes, values, goals, and practices that characterizes an institution or organization;

c: the set of values, conventions, or social practices associated with a particular field, activity, or societal characteristic.

By definition, UBMD is a culture, and compliance is a culture within that culture. The Compliance Plan is UBMD's set of shared attitudes, values, goals and practices that distinguish us as an organization. The Compliance Plan is, or should be, the characteristic features of our everyday existence, our way of life, in our workplace.

The UBMD Compliance Plan was created, and continues to grow, based on guidelines for an effective compliance program provided by the Office of Inspector General (OIG). The OIG's hospital guidance states that compliance efforts are designed to establish a culture that promotes prevention, detection and resolution of conduct that does not conform to federal and state law, and federal, state and private payor requirements, as well the hospital's policies.

As the UBMD website affirms:

- *We play a unique and vital role in the region: training the next generation of health care leaders while advancing standards of care for today's patients.*
- *We keep current on the very best practices and the latest advances in medicine, so [our patients] receive the most up-to-date care.*

To be successful with these affirmations, an effective compliance program is imperative. According to the OIG, an effective compliance program isn't just a plan written in a binder and set on shelf somewhere. It is essential to have a living, active compliance program based on our written Compliance Plan. An ineffective compliance program can lead to increased costs and inefficiencies to the patients, and puts UBMD at risk for violations, fraud, waste and abuse. One of the first things the OIG looks at during an investigation is the effectiveness of the compliance program; an ineffective program can lead to larger fines and other penalties.

We all need to promote a compliance culture within our practices where all UBMD providers and staff are committed to understanding and adhering to all rules, regulations, laws, and our Code of Conduct and compliance policies. If employees show a greater commitment to these things, they may feel less threatened, therefore less likely to compromise UBMD standards.

Some people may view compliance and compliance training as intimidating, overwhelming or even annoying. It really shouldn't be. As healthcare professionals, compliance is a necessary part of our jobs. By making compliance a part of your everyday routine, it becomes a familiar force of habit, and forms a stronger compliance culture: a culture of confidentiality, a culture of trust, a culture of integrity.

The stronger our compliance culture is, the more effective our compliance program is.

Cybersecurity: Phishing

From the HHS Office for Civil Rights (OCR) in Action

The following is an email we recently received from OCR regarding HIPPA Security Rule information that reinforces information we have provided in previous editions of this newsletter. Phishing has become a common way for scammers to attempt to obtain sensitive information such as usernames, passwords, and credit card information. The more aware you are, better!

Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information via electronic communication by impersonating a trustworthy source. For example, an individual may receive an e-mail or text message informing the individual that their password may have been hacked. The phishing email or text may then instruct the individual to click on a link to reset their password. In many instances, the link will direct the individual to a website impersonating an organization's real web site (e.g., bank, government agency, email service, retail site) and ask for the individual's login credentials (username and password). Once entered into the fake website, the third party that initiated the phishing attack will have the individual's login credentials for that site and can begin other malicious activity such as looking for sensitive information or using the individual's email contact list to send more phishing attacks. Alternatively, rather than capture login credentials, the link on the phishing message may download malicious software on to the individual's computer. Phishing messages could also include attachments, such as a spreadsheet or document, containing malicious software that executes when such attachments are opened. Phishing is one of the primary methods used to distribute malicious software, including ransomware.

"Individuals must remain vigilant in their efforts to detect and not fall prey to phishing attacks... "

Individuals must remain vigilant in their efforts to detect and not fall prey to phishing attacks because these attacks are becoming more sophisticated and harder to detect. Phishing attacks take advantage of popular holidays by impersonating messages from shipping vendors and ecommerce sites. Similarly, phishing attacks regarding tax refunds are common during tax season (March and April). A specific type of phishing attack, known as spear phishing, targets specific individuals within an organization. For example, a spear phishing attack could target an individual in the IT, accounting or finance department of an organization by impersonating the individual's supervisor and directing the individual to a malicious website or to download a file containing a malicious program. One of the primary methods of combating phishing attacks of all kinds is through user awareness. OCR included information on cybersecurity training and awareness programs in its July 2017 newsletter.[1]

Tips to avoid becoming a victim of a phishing attack include:

- Be wary of unsolicited third party messages seeking information. If you are suspicious of an unsolicited message, call the business or person that sent the message to verify that they sent it and that the request is legitimate.
- Be wary of messages even from recognized sources. Messages from co-workers or a supervisor as well as messages from close relatives or friends could be sent from hacked accounts used to send phishing messages.
- Be cautious when responding to messages sent by third parties. Contact information listed in phishing messages such as email addresses, web sites, and phone numbers could redirect you to the malicious party that sent the phishing message. When verifying the contents of a message, use known good contact information or, for a business, the contact information provided on its web site.
- Be wary of clicking on links or downloading attachments from unsolicited messages. Phishing messages could include links directing people to malicious web sites or attachments that execute malicious software when opened.
- Be wary of even official looking messages and links. Phishing messages may direct you to fake web sites mimicking real websites using web site names that appear to be official, but which may contain intentional typos to trick individuals. For example, a phishing attack may direct someone to a fake website that uses 1's (ones) instead of l's (i.e., a11phishes vs. allphishes).

Continued on Page 7

- Use multi-factor authentication. Multi-factor authentication reduces the possibility that someone can hack into your account using only your password. OCR's November 2016 cybersecurity newsletter included information on types of authentication.[2]
- Keep anti-malware software and system patches up to date. If you do fall for a phishing scam, anti-malware software can help prevent infection by a virus or other malicious software. Also, ensuring patches are up to date reduces the possibility that malicious software could exploit known vulnerabilities of your computer's or mobile device's operating system and applications.
- Back up your data. In the event that malicious software, such as ransomware, does get installed on your computer, you want to make sure you have a current backup of your data. Malicious software that deletes your data or holds it for ransom may not be retrievable. Robust, frequent backups may be the only way to restore data in the event of a successful attack. Also, be sure to test backups by restoring data from time to time to ensure that the backup strategy you have in place is effective.

There are many resources available to help people identify and avoid phishing attacks. For additional information, please visit the resources below.

- Federal Trade Commission (FTC) consumer information on phishing
  https://www.consumer.ftc.gov/articles/0003-phishing
- Federal Bureau of Investigation (FBI) information on spear phishing
  https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109
- Department of Homeland Security (DHS) video to protect against phishing attacks
  https://www.dhs.gov/science-and-technology/cyber-tip-become-cyber-savvyprotect-against-phishing-attacks

[1] https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf
[2] https://www.hhs.gov/sites/default/files/november-2016-cyber-newsletter.pdf

CONTACT US:

77 Goodell St., Suite 310
Buffalo, NY 14203

Fax: 716.849.5620

Lawrence C. DiGiulio, Esq.
Chief Compliance Officer
716.888.4705
larryd@buffalo.edu

Beverly A. Welshans, CHC, CPMC, CPC, CPCI, COC, CCSP
Director of Audit & Education
716.888.4702
welshans@buffalo.edu

Suzanne M. Marasi, CHC, CPC-A
Compliance Administrator
716.888.4708
smmarasi@buffalo.edu

UBMD COMPLIANCE HOTLINE: 716.888.4752

Report suspect fraud/abuse, potential problems,

or HIPAA concerns.

Ask questions or request guidance | Provide relevant information.

Remain anonymous if you wish | Non-retaliation policy will be adhered to.

(This is a voice mail box monitored during working hours. If there is an immediate threat to person or property, do not leave message; contact direct supervisor immediately!

Compliance Quarterly Quiz

To submit your quiz answers, please click link below:

2018 First Quarter Quiz

---

1. Which of the following is a reason for performing medical record audits?

   A. To protect against fraudulent claims and billing activity.
   B. To identify reimbursement deficiencies and opportunities for appropriate reimbursement.
   C. To stop the use of outdated or incorrect codes for procedures.
   D. All of the above are reasons for performing medical record audits.

2. All UBMD personnel - providers and staff - are required to complete a minimum of two hours of compliance training biennially (every two years).

   A. True
   B. False

3. Which of the follow is incorrect regarding student documentation of E/M services?

   A. Students may document services in the medical record.
   B. The teaching physician must verify in the medical record all student documentation or findings, including history, physical exam and/or medical decision making.
   C. Students may act as scribes during the same patient visit that they document their own actions.
   D. This change, allowing students to document E/M services, is part of a broader goal to reduce administrative burden on practitioners.

4. An ineffective compliance program can lead to increased costs and inefficiencies to the patients, and puts UBMD at risk for violations, fraud, waste and abuse.

   A. True
   B. False

5. All of the following statements are true, except:

   A. Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information.
   B. Messages from recognized sources such as co-workers, friends and family will never be phishing messages.
   C. Phishing messages could include attachments, such as a spreadsheet or document, containing malicious software that executes when such attachments are opened.
   D. Phishing messages could include links directing people to malicious web sites.