2022 1st Quarter
Volume 16, Issue 1

Compliance Quarterly

From the Compliance Office...

From the Compliance Office

HIPAA: Patient Right of Access

The Health & Human Services Office of Civil Rights (OCR) continues to enforce patient rights of access to medical records. We first brought OCR's patient right of access efforts to your attention during Compliance Week 2020 at which time there had been at least 10 enforcement actions. We reiterated the importance of Patient Right of Access in our 2020 4th quarter *Compliance Quarterly*, when the total of enforcement actions had risen to 14. In our 2021 1st quarter *Compliance Quarterly* we again reminded you of OCR's efforts as the 15th, 16th, 17th & 18th settlements were announced. With the resolution of two investigations announced on March 28, 2022, enforcement actions have now climbed to 27 since the initiative began.

It is important to remember that patients are permitted to review their records, obtain a copy of their records, or both. They also have a right to request that their records be changed or amended. Medical records must be provided to the patient in the format requested, whether they want paper or electronic (thumb drive), within 10 days of their initial request.

Compliance Training Updates

New Provider E/M & Documentation Training: **Required** for all newly hired providers. It also serves as a good refresher for not-so-new providers. This training is now available online by visiting the Education & Training page on the UBMD Compliance website (https://ubmd.com/about-ubmd/Compliance/Education-training.html). You may also call or schedule a Zoom meeting with Peter Rossow if you have questions, or would like to discuss anything with him.

Cultural Competency Training:

Some practices have received letters from 3rd party payers stating that NYS requires all Medicaid providers and staff to attest annually that cultural compliance training has been completed by all practice personnel. The Compliance Office has put together a PowerPoint presentation and quiz to meet this requirement. At this time it will be distributed to practices upon request. If you receive such a letter, please contact Sue Marasi, and she will provide you the training program and instructions.

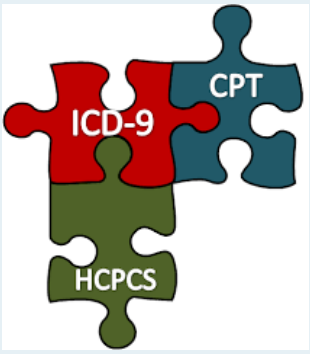
Mandatory Fraud, Waste & Abuse

Like last year, Mandatory Fraud, Waste & Abuse training will again be completed via PowerPoint program on our UBMD Compliance Office website. Directions will be sent out to practice Chairs, CFOs/PPAs and compliance liaisons by the end of the 2nd quarter. We ask that those parties ensure that the instructions are distributed to ALL practice providers and staff.

Inside this issue

HELP WANTED!!

We want you to be involved! If you have a question or topic you would like to see covered, general or specific practice-focused, in a future edition of the *Compliance Quarterly,* please contact Sue Marasi at: smmarasi@buffalo.edu



The Coding Corner

If you have any questions on this or other coding concerns, please contact Peter Rossow at: pvrossow@buffalo.edu 716-888-4702

HCC Coding Series

By: Peter Rossow, CPC, CPMA, Director of Audit & Education

Hierarchical Condition Category (HCC) coding is the risk adjustment model that is used by CMS for determining future healthcare costs associated to a specific patient. By coding chronic conditions to the highest level of specificity, a picture can be drawn of what healthcare resources will be needed in the future to treat the patient. Over the course of the next year, I will go in-depth on a few different HCC's, covering the clinical nature of the conditions, as well as proper coding and documentation of each. Let's begin!

Intracranial Hemorrhage (HCC145) & Ischemic Stroke (HCC146)

Cerebrovascular disease includes a variety of medical conditions that affect the blood vessels of the brain and the cerebral circulation. Arteries supplying oxygen and nutrients to the brain are often damaged or deformed in these disorders. The most common presentation of cerebrovascular disease is an ischemic stroke or mini-stroke and sometimes a hemorrhagic stroke. According to the Internet Stroke Center, stroke causes more than 140,000 deaths each year in the US, and the condition is the leading cause of serious, long-term disability in the country. For reimbursement purposes and also to provide better patient care, accurate documentation and correct ICD-10-CM codes are key to describe the patient's condition.

Symptoms and Risk Factors

The signs and symptoms of cerebrovascular disease depend on where the blockage occurs, and the extent of cerebral tissue affected. Blood flow in the brain can be restricted due to various reasons:

- The formation of clots may form (thrombosis)
- The narrowing of the vessels may narrow (stenosis)
- A blockage (embolism); or
- Bursting of a blood vessel (hemorrhage)

High blood pressure is a major risk factor for a cerebrovascular disorder such as a stroke. Other risk factors include older age, family history of cerebrovascular disease, obesity, diabetes, high cholesterol, atrial fibrillation, drug abuse, smoking, and high cholesterol. Men also have a higher risk.

A cerebrovascular disorder may present with any of the following symptoms:

- Severe and sudden headache
- Paralysis of one side (hemiplegia)
- Weakness on one side (hemiparesis)
- Abnormal or slurred speech
- Confusion
- Dizziness or nausea
- Vision problems
- Numbness
- Loss of balance
- Loss of consciousness

Diagnosis Coding

In ICD-10 CM, code category I60-63 should be utilized when the medical documentation indicates that an infarction or stroke has occurred. Coding of sequelae of stroke and infarction (ICD-10-CM category I69.-) also demands a level of detail often missing in medical records. There are specific codes which indicate the cause of the infarction, such as embolism or thrombosis, as well as the specific affected arteries. The sixth digit provides additional information which designates the affected side when applicable.

Continued on next page

Continued from page 2

ICD Codes	Stroke type
I60.-	Spontaneous subarachnoid hemorrhage
I61.-	Spontaneous intracerebral hemorrhage
I62.-	Spontaneous subdural hemorrhage
I63.0-I63.2	Thrombosis/embolus precerebral arteries
I63.3-I63.5	Thrombosis/embolus cerebral arteries
I63.6	Venous thrombosis
I63.8	Other specified cerebral infarction
I63.9	Unspecified cerebral infarction
G45.9	Transient cerebral ischemic attack, unspecified (TIA)
Z86.73	Personal history of TIA or cerebral infarct without residual deficits

When coding a stroke, infarction, or hemorrhage, seek answers to two questions. First, ask if the cerebral event is acute, or emergent. Second, find in the medical record details of the site, laterality, and type of stroke or infarction.

Acute CVA vs. History of CVA vs. CVA With Residual Deficits

Stroke is frequently miscoded. Errors include coding a stroke as a history versus a stroke with residual deficits, as well as coding a stroke as current when it is not. It is unlikely that a patient would have a definitive (ie, acute) stroke in an outpatient setting, allowing the provider to accurately document and code "stroke"; these conditions are diagnosed in the hospital after extensive examination and testing. Thus, acute CVA (ICD-10 category I60-63.-) is only to be used during the acute inpatient encounter. Once the patient is discharged, it is not appropriate to code for the stroke. Instead, you would code any and all residual deficits the patient has.

Patients who have had a stroke in the past may have residual deficits. This is what we would expect to see coded on the outpatient side. It is critical to carefully review the documentation in order to accurately capture these conditions. ICD-10-CM code Z86.73 is used to report personal history of transient ischemic attack (TIA) and cerebral infarction without residual deficits. Though there is no HCC associated with Z86.73, HCCs are present in many of the residual deficits of a cerebral infarction (ICD-10 category I69.-).

For example, a provider's documentation may state that a patient has had a stroke in the past. During the physical exam, the provider notes that the patient has right hemiplegia as a result of a previous stroke. It would be inappropriate to code Z86.73 in this case. Instead, you would use the code I69.351 to capture the current stroke sequela, hemiplegia and hemiparesis following cerebral infarction affecting the right dominant side. If the patient does not have any deficits, you can apply the ICD-10-CM code Z86.73.

The amount of specificity and detail available in ICD-10 CM makes complete and accurate documentation essential. Coders will need to thoroughly review the record in order to locate and assign the correct diagnosis code.

Stroke Coding and Documentation Tips

- If the patient's dominant side is not documented, assume the left side is non-dominant, except for ambidextrous patients. In ambidextrous patients, assume the affected side is dominant.
- Report any and all neurological deficits of a cerebrovascular accident that are exhibited anytime during a hospitalization, even if the deficits resolve before the patient is released from the hospital.
- Once the patient has completed the initial treatment for stroke and is released from acute care, report deficits with codes from I69 Sequelae of cerebral infarction. Neurologic deficits may be present at the time of the acute event or may arise at any time after the acute event.
- Codes I60-I69 should never be used to report traumatic intracranial events.
- Normally, do not report codes from I60-I67 with codes from I69. However, if the patient has deficits from an old cerebrovascular event and is currently having a new cerebrovascular event, both may be reported.
- If a patient is diagnosed with bilateral nontraumatic intracerebral hemorrhages, report I61.6 Nontraumatic intracerebral hemorrhage, multiple localized. For bilateral subarachnoid hemorrhage, assign a code for each site. Categories I65 and I66 have unique codes for bilateral conditions.
- Also code any documented atrial fibrillation, CAD, diabetes, or hypertension as these comorbidities are stroke risk factors.
- Non-specific codes (ICD-10-CM categories I63.8 and I63.9) should not be used when the cause/site of the stroke is known.

HIPAA: Protecting Yourself from Cyberattacks

By: Sue Marasi, CHC, CPCA, Compliance Administrator

In 2021, healthcare organizations were found to be especially vulnerable to security breaches via cyberattacks, malware, and ransomware, especially during the Covid pandemic, at facilities across the country. The number of security breaches in the healthcare industry increased by about 70% and reported losses exceeding $4 billion over the previous year.

The FBI, which continued to issue cybersecurity warnings, suggested that organizations should institute a proactive strategy by searching for signs of threat activity to prevent attacks before they occur or to minimize damage should a successful attack occur. Suggested strategy included providing patients with access to their PHI as required and avoiding or reducing inappropriate and inadvertent disclosures of PHI by workforce members through improved training of workforce members. Our Compliance Office has worked to adhere to these suggestions.

In addition, on March 24, 2022, UB's Vice President and Chief Information Officer Brice Bible sent an email to the University community with direction on how to protect yourself from cyberattacks. The content of his email is as follows:

> *Dear UB community member,*
>
> *A growing concern surrounding the tensions in Europe is the increased risk of cybersecurity attacks throughout the globe.*
>
> *Bad actors from all over the world are opportunistic. Fraudulent fundraising campaigns for Ukraine and other similar attacks will continue to be prevalent.*
>
> *With that in mind, it's important to remain vigilant at this time as we monitor this delicate situation.*
>
> ***What can you do to stay cyber-safe?***
>
> *Simply put, practice the same cyber hygiene as always, but with renewed determination:*
>
> ***Stay watchful for incoming phishing attacks and report them as soon as received.*** *If you are the victim of a phishing attack, immediately change your UBIT password and contact the UBIT Help Center for further assistance via buffalo.edu/ubit/help or 716-645-3542.*
>
> ***If you observe something unusual, submit a request to your IT support staff or UB's Information Security Office for review.***
>
> ***Review UBIT's latest safe computing tips and guidance at buffalo.edu/ubit/safe.***
>
> ***If Duo prompts you to authorize a login attempt you did not initiate, use the Duo Mobile app to deny the request and flag it as fraudulent.*** *In addition, immediately change your UBITName password.*
>
> ***Confirm that critical data is adequately and securely backed up.*** *Take advantage of UBbox or OneDrive storage. UB faculty and staff: contact your departmental IT support if you have questions on how to best back up your data.*
>
> *Thank you for your diligence and attention to this matter.*

If you think you may have been a victim of attack and are still unsure of what to do, or if you do not have a UBIT, immediately contact our UBMD Compliance Office for direction.

General Compliance: Cyberattack Threats & Breaches

By: Sue Marasi, CHC, CPCA, Compliance Administrator

Building on the previous article, because the healthcare industry has been a main target of cyberattacks, it makes sense to further discuss some specifics of threats including breaches, hacking, phishing, and cybersecurity/malware/ransomware.

According to a 2022 Breach Barometer report by healthcare compliance analytics company, Protenus, Inc., there were 40.7 million patient records breached in 758 incidents in 2020; in 2021, that number increased to 50.4 million in 905 incidents. Keep in mind, this refers to all *known* healthcare data breaches; the volume and impact of breaches continues to be underreported. In 2021 60% of data breach incidents were reported or disclosed by providers, with the remainder being reported by health plans, clearinghouses, business associates/third-party, and "other."

The single largest breach reported in 2021 was a hacking incident involving an IT business associate of a children's health plan. As many as 3.5 million individuals were affected. Hackers were able to access information including full names, birth dates, email addresses, phone numbers, addresses, Social Security numbers, financial information, family relationships and secondary insurance data.

Incidents involving Business Associates accounted for 146 of the incidents in 2021. 109 of those (75%) involved hacking. This highlights the importance of having signed Business Associate Agreements with all entities your practice works with that have, or could possibly have (ie: cleaning company), access to ePHI.

According to the Protenus report, 2021 marked the sixth consecutive year that hacking incidents were on the rise. Eight out of the twelve largest health data breaches in 2021 were hacks, six of which were of providers' data. Three others were via ransomware, and one was "unknown;" all four of those were also providers' data.

According to HHS, phishing is the number one method of cyberattacks, responsible for 90% of security breaches. Recovering from damage caused by a phishing attack costs an average of $8 million. It remains a serious compliance threat. Phishing tricks individuals into directly revealing sensitive information, such as login credentials, or infects your computer with a virus (ie: malware, ransomware), by posing as a legitimate, reputable business or person. Most commonly phishing occurs with a fraudulent email solicitation providing a deceptive link or malicious "advertisement" embedded in an email or website.

While many system safeguards are kept up to date by our IT personnel to prevent cyberattacks, there are many ways you can and should help to defend against them as well.

- Make sure signed Business Associate Agreements (BAAs) are obtained and kept on file for all business associates that have, or could possibly have, access to ePHI.
- Any laptops and mobile devices that contain ePHI should be encrypted and password protected.
- Internal controls and security procedures should be followed by all providers and staff at all times. Do NOT share passwords. Always log off/lock laptops and desktops when you walk away from them.
- Before you click on any link or share any sensitive information:
  - ⇒ **CHECK** if you recognize the sender. Were you expecting this email? Be aware of spoof email addresses that look legitimate. Look up the website or phone number for the company or person behind the email.
  - ⇒ **ASK** yourself if the email is asking for login credentials or personal information. Is the greeting/signature generic or lacking contact information? Are there misspellings in the content? If so, be very suspicious. NEVER share login credentials with anyone, and validate contact information using a secondary source.
  - ⇒ **TALK** to someone. If you are unsure, contact the Compliance Office, a supervisor or an IT representative to help figure out if the email is real or a phishing attempt.

"Example is not the main thing in influencing others. It is the only thing."

~ Albert Schweitzer

OIG: By the Numbers

By: Sue Marasi, CHC, CPCA, Compliance Administrator

The Fall 2021 Semiannual Report to Congress was issued by the OIG Department of Health and Human Services on 4/2/21. The Semiannual Report describes the OIG's work identifying significant risks, problems, abuses, deficiencies, remedies, and investigative outcomes relating to the administration of HHS programs and operations disclosed during the period of 4/1/2021 through 9/30/21.

The following is a summary of OIG's outcomes for the **entire 2021 fiscal year** (10/1/20-9/30/21):

Audit Reports Issued	162
Evaluations Issued	46
Expected Audit Recoveries	$787.29 Million
Questioned Costs	$1.17 Billion
Potential Savings	$1.24 Billion
New Audit & Evaluation Recommendations	506
Expected Investigative Recoveries	$3.0 Billion
Criminal Actions	532
Civil Actions	689
Exclusions	1,689

In addition, the OIG and law enforcement partnered in a 6 week federal law enforcement action to combat COVID related schemes to fraudulently bill Medicare for medically unnecessary testing and medical equipment. The action resulted in criminal charges against 138 defendants, including more than 42 doctors, nurses, and other licensed medical professionals, for more than $1.4 billion in alleged losses.

These numbers are real, and should illustrate to everyone the importance of being aware of your documentation, coding, billing and general compliance at all times.

UBMD Compliance Office Website: https://ubmd.com/about-ubmd/Compliance.html

CONTACT US:

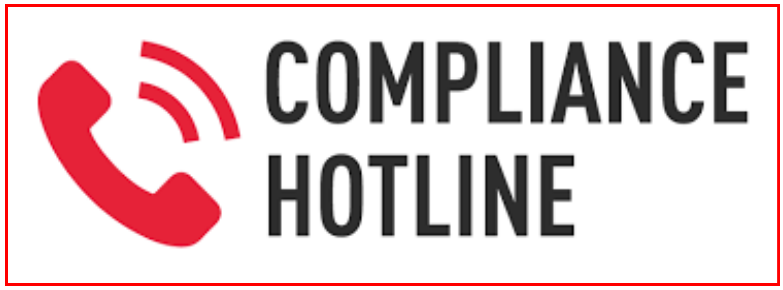
77 Goodell St., Suite 310
Buffalo, NY 14203

Fax: 716.849.5620

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

Peter V. Rossow, CPC, CPMC
Director of Audit & Education
716.888.4702
pvrossow@buffalo.edu

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



UBMD COMPLIANCE HOTLINE: 716.888.4752

CONFIDENTIAL!

Report known or suspected fraud/abuse, HIPAA concerns, or other potential problems.

Ask questions or request guidance | Provide relevant information

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

CLICK HERE FOR PRINTABLE FLIER: Hotline Flier

(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:

2022 First Quarter Quiz

---

1. Stroke risk factors (eg. Afib, CAD, DM), if documented, should be coded in addition to the stroke code.

   A. True
   B. False

2. A 53-year-old right handed man is admitted into the hospital and diagnosed with cerebral infarction, unspecified (ICD-10-CM code I63.9). At the 3-week post-discharge follow-up appointment for the cerebral infarction, the office visit note states the patient had a stroke and has a residual deficit of ataxia. What is the most appropriate code(s) for this scenario?

   A. I69.053
   B. G45.8
   C. I69.393
   D. I69.398, R27.0

3. Which of the following statements is incorrect?

   A. Patients are permitted to review their records, obtain a copy of their records, or both.
   B. Medical records must be provided to the patient in the format requested, whether they want paper or Electronic (ie: thumb drive).
   C. Records must be provided to the patient within 10 days of the initial request.
   D. Patients do not have a right to request that their records be changed or amended.

4. According to HHS, phishing is the number one method of _____.

   A. Providing patients with their records.
   B. Safeguarding ePHI records.
   C. Cyberattacks.
   D. Putting dinner on the table.

5. It is not necessary for laptops and mobile devices containing ePHI to be encrypted and password protected.

   A. True
   B. False