2019 4th Quarter
Volume 13, Issue 4 &
2019 1st Quarter
Volume 14, Issue 1

Compliance Quarterly

From the Compliance Office...

Combined Newsletter

Due to various circumstances, we have combined the 2019 4th Quarter and 2020 1st Quarter newsletters. The attached quiz is 10 questions so that you can receive .50 hour training credit with successful completion.

Newsletter Topics

In the *Compliance Quarterly,* we focus on currently relevant Compliance & HIPAA topics, regulatory updates, and helpful tips. If anyone has a topic you would like to see covered, general or practice-focused, in a future edition of *Compliance Quarterly,* please contact Sue Marasi (smmarasi@buffalo.edu).

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.***

****Available for one-on-one sessions. Please contact Bev Welshans to set up a session.***

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

2020 Dates: 6/16, 8/18, 9/15, 10/20, 11/17
(There will be no sessions in July or December.)

**** Due to the Covid-19 situation, Lunch-n-Learn dates may need to be rescheduled.***

Inside this issue

Training Questions

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

The SHIELD Act

By: Sue Marasi, CHC, CPCA, Compliance Administrator

On July 25, 2019, the Governor of New York signed the Stop Hacks and Improve Electronic Data Security (SHIELD) Act into law. The SHIELD Act broadens the definitions of "private information" and "data breach" that existed in the New York data breach notification law, updates notification procedures that must be followed in the event of a breach of private information, and requires organizations to develop, implement and maintain administrative, technical and physical safeguards to protect the data of New York residents.

The SHIELD Act defines a security breach as unauthorized access to private information, even if an unauthorized entity only views information and documents, without downloading or copying it.

There are two types of data protected by the SHIELD Act: personal information and private information. Personal information is any information that can be used to identify a person, such as name, number, personal mark or other identifier. Private information is certain types of computerized data such as social security number, drivers license or other ID card number, account number, debit/credit card numbers, biometric information (finger prints, voice print, retina or iris image), and login information (username, email address, password, and security questions/answers).

As stated above, organizations are required to develop and maintain administrative, technological and physical safeguards as part of a written information security program. Reasonable safeguards include the following:

1. Administrative
   - Designate employee(s) to coordinate security, and update safeguards as necessary;
   - Identify reasonably foreseeable internal and external risks;
   - Assess the adequacy of safeguards that are in place;
   - Train & manage employees in security procedures;
   - Require service providers/vendors, via contract, to maintain safeguards.
2. Technical
   - Assess risks in network and software design;
   - Assess risks in information processing, transmission and storage;
   - Regularly test and monitor controls, systems and procedures;
   - Detect, prevent & respond to attacks or system safeguards.
3. Physical
   - Assess the risks of information storage and disposal;
   - Detect, prevent & responds to intrusions;
   - Protect against unauthorized access or use of private information during/after data collection, transmission & destruction.

By now, you have surely noticed the similarities between New York's SHIELD Act and the Federal HIPAA and HITECH regulations. Those similarities are likely why entities that are compliant with HIPAA and HITECH are also deemed compliant under the SHIELD Act. There is, however, an additional point that needs to be stressed when it comes to data breach notifications and penalties that go above and beyond HIPAA/HITECH requirements.

Should a breach occur, under the SHIELD Act, the organization is obligated to give notice to the individual(s) affected, via written, electronic or phone communications, or other notification method such as public posting or via statewide media. Notifications should be done "without reasonable delay." **The organization must also inform the State Attorney General about data disclosure.** While organizations are not required to issue duplicate notifications when data breach notification is required under another regulation such as HIPAA or HITECH, they are still required to, notify the NYS Attorney General, NYS Department of State Division of Consumer Protection, and NYS Division of State Police. Because of this, failure to report a breach could result in a violation of multiple regulations (eg. NY SHIELD Act and HIPAA), potentially triggering penalties under each regulation.

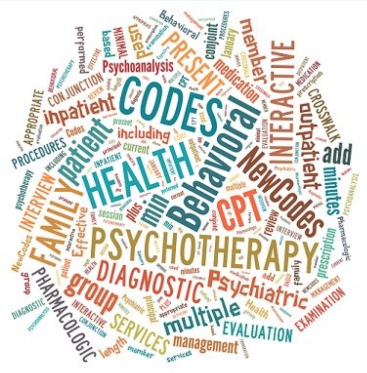
The State Attorney General can bring legal action anytime within 3 years of the date when the AG becomes aware of the violation, or the date when the entity provides notice of the breach, whichever is first. Once 6 years have passed after the breach itself, provided the company has not been hiding it, no action can be brought.

Continued on Page 3

Continued from page 2

Finally, the penalties for violating the SHIELD Act vary depending on the type of violation:

1. Reasonable safeguard requirement violation
   - Up to $5,000 per violation.
2. Knowing and reckless violation
   - The greater of $5,000 or up to $20 per instance with a cap of $250,000.
3. Not knowing or reckless violation
   - Damages for actual costs or losses incurred by a person entitled to notice, including consequential Consequential financial losses.



Highlights of CPT-4 Changes for 2020

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

The American Medical Association's (AMA's) 2020 update of the CPT code set comprises of 394 code changes, including 248 new codes, 71 deletions, and 75 revisions. The 2020 CPT code changes became effective on January 1, 2020. Here are some of the highlights and implications of the updates:

The Coding Corner

Six new CPT codes to report e-visits: Electronic visits (e-visits) help patients who would otherwise find it difficult to pay for medical care or have to travel long distances. Digital health tools address this concern by allowing patients and physicians to communicate asynchronously and outside of office settings.

In 2020, there are 6 new CPT codes for reporting a range of digital health services including e -visits through secure patient portal messages. 99421, 99422 and 99423 describe patient-initiated digital communications with a physician or other qualified health professional. 98970, 98971 and 98972 represent patient-initiated digital communications with a nonphysician health professional.

Two new codes for home blood pressure monitoring: New codes 99473 and 99474 will allow reporting self-measured blood pressure monitoring. Tracking blood pressure at home helps patients take an active role in the process and enables physicians to better diagnose and treat hypertension.

Good news for Orthopaedics, with new codes to cover "dry needling" and drug delivery devices. Two new codes, 20560 Needle insertion(s) without injection(s), 1 or 2 muscle(s), and 2056 for 3 or more muscles recognize the importance and use of "dry needling." Several new codes were added to reflect the services involved in mixing and preparing antibiotics (or other therapeutic agents) for delivery device; examples are: beads, nails, spacers. These codes are not to be used for fabricated devices. They are add-on codes used in addition to the primary procedure: +20700 Manual preparation and insertion of drug-delivery device(s), deep (eg. subfascial), +20701 Removal (deep), +20702 Manual preparation and insertion intramedullary),+20703 Removal (intramedullary), +20704 Manual preparation and insertion (intra-articular) and +20705 Removal of drug-device(s), intra-articular.

Updates for health and behavior assessment and intervention services: New codes 96156, 96158, 96164, 96167and 96170, and add-on codes 96159, 96165, 96168, and 96171 for health and behavior assessment and intervention services will replace six older codes. According to the AMA, this update is intended to "more accurately reflect current clinical practice that increasingly emphasizes interdisciplinary care coordination and teamwork with physicians in primary care and specialty settings."

Please feel free to contact
Bev with any questions:
welshans@buffalo.edu
888-4702

"A 'No' uttered from deepest conviction is better and greater than a 'Yes' merely uttered to please, or what is worse, avoid trouble."

~ Mahatma Gandhi

Continued from page 3

Enhancements for reporting long-term electroencephalographic (EEG) monitoring services (95700-95726): Four older codes have been deleted to make way for 23 new codes for long-term electroencephalographic (EEG) monitoring services. According to the AMA, the new codes provide better clarity around the services reported by a technologist, a physician, or another qualified health care provider. The codes 95700-95716 represent EEG technologist services, and codes 95717-95726 represent professional services.

Significant enhancements for cardiovascular coding: Codes have been updated to include imaging guidance or to provide greater specificity. For example, code 33275 changed from Transcatheter removal of permanent leadless pacemaker, right ventricular to Transcatheter removal of permanent leadless pacemaker, right ventricular, **including imaging guidance (eg: fluoroscopy, venous ultrasound, ventriculography, femoral venography), when performed.** Code 33860 changed from Ascending aorta graft, with cardiopulmonary bypass, includes valve suspension, when performed, to Ascending aorta graft, with cardiopulmonary bypass, includes valve suspension, when performed; **for aortic dissection,** and the new code, •33859 for the same procedure **for aortic disease other than dissection (e:, aneurysm**).

This area also sees several new category III codes reflecting advances in Transcatheter procedures: 0345T Transcatheter mitral valve repair, 0483T Transcatheter mitral valve implantation/replacement (TMV), 0544T Transcatheter mitral valve annulus reconstruction, and 0569T Transcatheter tricuspid valve repair.

Several new category III codes have also be added for Substernal Implantable Cardioverter-Defibrillator devices: 0571T Insertion or replacement system, 0572T Insertion electrode, 0573T Removal electrode, 0574T Repositioning, and 0575T Programming.

Gastroenterology sees revisions to Hemorrhoidectomy codes and addition of new pelvic packing codes. Two hemorrhoid codes been revised: 46945 Hemorrhoidectomy, internal, by ligation other than rubber band; single hemorrhoid column/group, **without imaging guidance**, and 46946 two or more hemorrhoid columns/groups, **without imaging guidance**. One new code has been added: ●46948 Hemorrhoidectomy, internal, by transanal hemorrhoidal dearterialization, two or more hemorrhoid columns/groups, including ultrasound guidance, with mucopexy, when performed.

Two new codes have been added for pelvic packing: 49013 Preperitoneal pelvic packing for hemorrhage associated with pelvic trauma, including local exploration, and 49014 Re-exploration of pelvic wound with removal of preperitoneal pelvic packing, including repacking, when performed.

Ophthalmology also underwent revisions of existing codes and addition of new codes: Revision of code 66711 to Ciliary body destruction; cyclophotocoagulation, endoscopic, **without concomitant removal of crystalline lens.** Current cataract extraction codes 66982 and 66984 were revised to **without endoscopic cyclophotocoagulation**. Two new corresponding cataract extraction codes were added: 66987 and 66988 for these 2 methods **with endoscopic cyclophotocoagulation.**

Other approved CPT changes for 2020 include two new vaccine codes 90694 to report a quadrivalent inactivated-adjuvanted influenza virus vaccine, and 90619 Meningococcal conjugate vaccine, serotypes A,C,W,Y, quadrivalent, tetanus toxoid carrier (MenACW-T) for IM use.

Gynecology sees the addition of two category III codes: 0567T to report transcervical bilateral permanent fallopian tube occlusion, and 0568T to report the separate introduction of saline for confirmation of occlusion via sonosalpingingraphy.

These are a few of the 2020 CPT4 changes. The list is not all-inclusive and you should always review the CPT4 manual for changes specific to your area of practice. There are numerous guidelines for use of particular codes too extensive for printing here. As always, review the coding guidelines prior to using any code.

I am always available should you have questions on these or any other coding issues.

General Compliance: 2019 OIG Semiannual - Report By the Numbers

By: Sue Marasi, CHC, CPCA, Compliance Administrator

The Department of Health and Human Services (HHS), Office of Inspector General (OIG) *Semiannual Report to Congress* summarizes OIG activities for all of FY 2019. More than $819 million is expected to be recovered from audits for FY 2019, and approximately $5.04 billion is expected from investigative recoveries for criminal actions, civil and administrative settlements, civil judgments and administrative actions by the OIG. In addition, in FY 2019, OIG:

- Brought 809 criminal actions against individuals or organizations engaging in crimes against HHS programs and the beneficiaries they serve;
- Brought 695 civil actions including false claims filed in Federal district court, civil monetary penalty settlements and administrative recoveries related to provider self-disclosure matters;
- Excluded 2,640 individuals and entities from participation in Medicare, Medicaid and other Federal health care programs.

The semiannual report also highlights OIG achievements and activities for the second half of the fiscal year (April 1, 2019 through September 30, 2019). Some of the areas the OIG focused its efforts on during this time include:

- Preventing opioid misuse and promoting access to treatment;
- Fighting fraud to protect Medicare and Medicaid programs;
- Protecting beneficiaries from abuse, neglect and unsafe conditions;
- Promoting access to high quality care;
- Safeguarding the security and integrity of medical research.

During this second half period, the OIG issued 91 audit reports and 36 evaluation reports. This work resulted in identifying nearly $323 million in expected recoveries, and over $666.5 million in costs questioned by the OIG because of an alleged violation, costs not supported by adequate documentation, or unnecessary or unreasonable intended purpose of expenditure of funds.

The semiannual report reminds us that OIG investigates allegations of fraud, waste and abuse in all HHS programs. Their largest area of focus is matters related to the Medicare and Medicaid programs, such as:

- Patient harm;
- Billing for services not rendered;
- Medically unnecessary services;
- Upcoded services;
- Receipt of kickbacks (including illegal payments to patients for involvement in fraud schemes, and illegal referral arrangements between physicians and medical companies).

According to the OIG, one of the most common types of fraud that has been carried out against Medicare, Medicaid and other Federal health care programs involves filing false claims for reimbursement. During this semiannual reporting period, the OIG reported:

- 353 criminal and 357 civil actions against individuals or entities that engaged in healthcare-related offenses;
- Over $1.47 billion in HHS investigative receivables, and more than $1.13 billion in non-HHS investigative receivables, including civil and administrative settlements or civil judgments related to Medicare, Medicaid, and other Federal, State and private healthcare programs.

Investigative outcomes can result in incarceration, restitution, fines, penalties, forfeitures, assessments, and exclusion of individuals or entities from participation in all Federal health care programs.

Continued on page 6

Continued from page 5

Many healthcare providers elect to settle cases before going to litigation. Oftentimes, as part of these settlements, providers agree to enter into Corporate Integrity Agreements (CIAs) with the OIG to avoid exclusion. Under a CIA, the provider commits to establishing a program to ensure future compliance with Federal health care program rules. CIAs are designed, in part, to prevent future fraud. The provider's compliance with these agreements is closely monitored, and penalties may be imposed on entities that fail to comply with the requirements of their CIAs.

The following is a true medical necessity case example provided by the OIG that illustrates the cost associated with non-compliance:

In Kansas, a physician and a medical group entered into a settlement agreement with the United States to resolve allegations that they submitted, or caused to be submitted, false claims to Medicare, TRICARE, and the Federal Employees Health Benefits Program for cardiac stent procedures that were not medically necessary. The physician and medical group agreed to pay $5.8 million to resolve the allegations. In addition, as part of the settlement, the physician also agreed to be excluded for three years.

Finally, the OIG shared the activity of their Hotline complaints for the period of 4/1/2019-9/30/2019. During this semiannual reporting period, the OIG reported expected recoveries of $8million as a direct result of cases originating from hotline complaints.

• Contacts to Hotline, including callers seeking information:	81,762
• Total tips evaluated:	21,146
• Tips referred for action:	15,419*
• Closed; no basis provided for further action:	5,850
• Closed; no HHS violation:	716

* Tips referred for action came from phone calls (5,431); OIG website (7,695); letters/faxes (1,112); other (1,181).

This illustrates that people can and do report when they see non-compliance. This is why we encourage our UBMD providers and staff to report known or suspected fraud or other concerns to our own UBMD Compliance Hotline. Better to investigate and resolve any potential problems before they become more serious.

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:

2019 Fourth/2020 First Quarter Quiz

1. ________ requires organizations to develop, implement and maintain administrative, technical and physical safeguards to protect the data of New York State residents.

   A. False Claims Act
   B. Stark Law
   C. SHIELD Act
   D. Antikickback Statute

2. The SHIELD Act only protects personal information, such as name, number, personal mark or other identifier.

   A. True
   B. False

3. Although entities that are compliant with HIPAA and HITECH are also deemed compliant under the SHIELD Act, they must also inform the NYS Attorney General about data disclosure

   A. True
   B. False

4. Which codes are used to describe patient-initiated digital communications with a physician or other qualified health professional?

   A. 99421, 99422, 99423
   B. 98970, 98971, 98972
   C. 99473, 99474
   D. All of the above

5. According to the AMA, the code update for health and behavior assessment and intervention services is intended to more accurately reflect current clinical practice that increasingly emphasizes interdisciplinary care coordination and teamwork with physicians in primary care and specialty settings.

   A. True
   B. False

QUIZ CONTINUED ON NEXT PAGE

Compliance Quarterly Quiz

Continued from Page 7

6. Which of the following statements is correct regarding EEG monitoring?
   A. Four older codes have been deleted to make way for 23 new codes for long -term EEG monitoring services.
   B. 95700-95716 represent EEG technologist services.
   C. 95717-95726 represent professional services.
   D. All of the above are correct.

7. Cardiovascular coding has no significant changes for 2020.

   A. True
   B. False

8. Approximately $5.04 billion is expected from criminal actions, civil and administrative settlements, civil judgments and administrative actions by the OIG for Fiscal Year 2019.

   A. True
   B. False

9. The OIG's largest area of focus is matters related to the Medicare and Medicaid programs including which of the following?
   A. Billing for services not rendered.
   B. Medically unnecessary services.
   C. Upcoded services.
   D. All of the above.

10. Which of the following statements is true?

    A. One of the most common types of fraud carried out against Medicare, Medicaid and other Federal health care programs involves filing false claims for reimbursement.
    B. Investigative outcomes can result in incarceration, restitution, fines, penalties, forfeitures, assessments, and exclusion of individuals or entities.
    C. Both A and B are true.
    D. None of the statements are true.