SAINT LOUIS UNIVERSITY
OFFICE OF UNIVERSITY COMPLIANCE

Summer 2018 Compliance Newsletter

Annual Compliance Training

Every year, billions of dollars are improperly spent because of fraud, waste, and abuse (FWA). Federal guidelines and our third-party contracts insist that every individual complete annual FWA and General Compliance Training. CMS does not distinguish employment status or contracting terms. Their definition includes every employee, temporary employee, volunteer, consultant, governing board member, and downstream entity that support (directly or indirectly) the healthcare encounter.

Every member of SLU's HIPAA-defined workforce, which includes all individuals affiliated with the clinical departments along with ITS and General Counsel, are required to complete the training modules. This includes full-time, part-time, adjunct and emeritus faculty, per diem, as well as volunteer faculty and staff.

This online education module provides an overview of the current healthcare compliance climate including the prevention and detection of fraud, waste and abuse, SLU's Compliance program, updated information regarding HIPAA and Information Security, Research Compliance, Conflicts of Interest, Export Controls, Contracting Basics, and Risk Management.

The 2018 Annual Compliance Update will take approximately one hour to complete. This includes watching 2 videos and answering a number of questions after each video. The update must be completed by August 31, 2018. The modules can be found after August 1st at myslu.slu.edu/home under Compliance Requirements.

Employees who do not complete the training module by the deadline will have their access to myslu.edu blocked until they have completed the module.

2018 Billers' Meeting Schedule

All meetings will be from 10:00-11:00am
Law Clinic Annex, 321 Spring Ave

July 10
August 14
September 11
October 9
November 13
December 11

The CODING CORNER

Diagnosis Sequencing

Diagnosis Sequencing has been a focal point since being included in the 2016 OIG work plan. Payers have started to communicate guidance regarding denials based on diagnosis codes.

Recently, Missouri Care issued communications which read “New or established Emergency Department E&M services higher than a level 3 with diagnosis ‘without abnormal findings’ may be denied.”

It is important to sequence your diagnoses in the order of importance. The most important/ relevant diagnosis should be listed first.

Example: You are a cardiologist and you are seeing a patient in the Emergency Room for acute onset chest pain with a diagnosis of acute anterior wall myocardial infarction. You would not code high blood pressure as your first diagnosis. This is a lower acuity problem and should be listed lower in your list of pertinent diagnoses for this visit.

International Travel Requirements

As summer approaches, here are some important reminders for international travelers.

No University equipment:
Technology purchased with university funds cannot be taken to the following countries: Albania, Armenia, Azerbaijan, Belarus, Cambodia, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam. If you are planning a trip to these countries for university business, please contact the Export Control Officer. To begin the process of reserving a clean, loaner laptop, contact the service desk at 977-4000. While university technology is not allowed in Iran, Sudan, N. Korea, and Cuba, additional travel and license restrictions apply to these four countries. If you have plans to travel to these countries, please contact the Export Control Officer immediately.

University equipment:
University technology is allowed to be taken freely to the remainder of the world’s countries after the traveler files a TMP with the Export Control Officer. *A TMP is required for both business and personal trips for University owned equipment.* In addition, ITS now requires a VPN to access SLU systems while traveling internationally. Contact the service desk to have a VPN installed on your machine. Contact the Export Control Officer to begin the process to file a TMP for the technology you wish to take on your next international trip.

For additional questions or concerns, please contact the Export Control Officer:
Michael Reeves
Michael.reeves@health.slu.edu
977-5880

Epic Access for Research Site Monitors

Most research agreements allow outside entities to regularly visit the University to monitor or audit study site documentation, including clinical research subject data. The site monitors represent regulatory oversight bodies, such as the FDA, Clinical Research Organizations, IRBs, and sponsors and their purpose varies, although human subject safety and protocol compliance are always a priority.

The sponsor develops a Monitoring Plan that identifies the frequency and duration of their periodic monitoring visits for the purpose of evaluating the way the study is being conducted and to perform source document verification. Be familiar with the contract agreements, as they should contain the sponsors' expectations for access to the research subjects' Protected Health Information (PHI) during those visits. Authorization for such access is included in the Informed Consent Document which specifically allows site monitors to review relevant PHI for source document verification of research data.

SLUCare's EHR Printing Policy requires that we strictly observe and protect the patients' PHI, and states that it should not be printed unless absolutely necessary for treatment, payment, or operational purposes. Therefore, we discourage printing medical records to paper as we are not able to vouch for the absolute security of our patients' data after it has been released to the monitor. Furthermore, general system access to Epic will not be granted as it exposes all patient data, and not just the PHI of identified research subjects.

There are multiple options for providing access to site monitors of patients' electronic medical records maintained in Epic. One option is for an authorized member of the research team to sit next to the site monitor. The SLU employee would access EPIC using their personal credentials and would navigate every keystroke to ensure restricted access was maintained.

There is also the potential to utilize an EpicCare Link account that allows for secure web based, read-only access. Viewable information can be specifically limited to qualifying elements of the patient's chart, such as a certain period of time (site visit dates). For more information, email the EpicCare Link team at carelinkaccess@health.slu.edu.

A final alternative for site monitor access is to request a formal release of information from SLUCare's Health Information Management / Release of Information team. The HIM/ROI team can create a downloaded file using the "Inspector Feature" of Epic that will include only the desired charts, time frames, etc. The PDF file can be viewed within Epic using a security key (with expiration date) that allows for viewing within a specified period of time. HIM will need to have a reasonable lead time to assemble the prepared data, at least two weeks prior to the site visit. They will need a list of the patients' names, medical record numbers, dates of birth, and other specific parameters relevant to the sponsored research. Viewing of the data can be performed using the "Inspector Kiosk" computer set up in the HIM Department.

We welcome your questions at SLUcompliance@health.slu.edu.

Guidance for Preventing Misdirected Disclosure of Paper After Visit Summaries (AVS)

Prevent misdirected disclosures by always verifying information, every time. The single most important step to take, the one that will prevent misdirection of an AVS every time, is simply to look at the document and verify what you are about to hand the patient is the correct AVS. You may even need to ask the patient their name again if you are in doubt. Never assume that another coworker reviewed the AVS for accuracy before it came to you. Once it is in your hands, it becomes your responsibility. Never routinely assume that the AVS in your hands is for the patient standing in front of you. Look at the patient's name on the document to ensure you are handing it to the correct patient and that it is only that patient's AVS, every time.

If a misdirected disclosure is discovered, react quickly. If a mistake is discovered while the receiving party is still in the building, immediately ask for the AVS and exchange it for the correct copy. If the receiving party has already left the building, there are a few options you may choose:

- You may call and request acknowledgement that they will destroy the misdirected document. Inform the patient that your office will mail them the correct copy if desired.
- If they have an appointment soon, they may bring it back to you and you can give them the correct copy in office.
- You may mail them a prepaid envelope, along with the correct copy and ask that they send the mistakenly disclosed copy back to your office.

The sooner you act, the less the likelihood that someone will view the patient's PHI. After you've taken steps to mitigate the problem, it is important to refresh yourself and all parties at fault with the relevant SLU policies to prevent this type of incident in the future. Non-compliance is not only a major risk to patient privacy and to the reputation of SLU and SLUCare, but it can lead to disciplinary action against repeat offenders as well.

After the incident is discovered, contact Compliance. It is important to notify University Compliance as soon as possible after an incident of misdirected disclosure is discovered. This can be done by emailing Privacy Officer, Ron Rawson at ron.rawson@health.slu.edu or Privacy Analyst, Christian Allen at christian.d.allen@health.slu.edu. You may also call 314-977-5545 for assistance. There may be additional steps that compliance needs to take to ensure the patient's privacy is protected and to ensure proper recordkeeping and reporting.

Department of Justice
Office of Public Affairs

Original date: Thursday, March 29, 2018

Michigan Home Health Agency Assistant Director of Nursing Sentenced to Three Years in Prison for Role in $1.6 Million Health Care Fraud Scheme

The assistant director of nursing of a Michigan home health agency was sentenced to 36 months in prison today for his role in a scheme involving approximately $1.6 million in fraudulent Medicare claims for home health services that were procured through the payment of kickbacks, and that were medically unnecessary and not provided.

The 3/29/2018 DOJ Announcement stated that Juan Yrorita, 63, of Sterling Heights, Michigan, was sentenced and ordered to pay $1,524,952 in restitution, jointly and severally with his co-conspirators, and to forfeit $49,823. After four days of trial, Yrorita pleaded guilty on Nov. 29, 2017 to one count of conspiracy to commit health care fraud and wire fraud.

As part of his guilty plea, Yrorita admitted that his co-conspirators at Anointed Care Services (Anointed), a Detroit-area home health agency, paid kickbacks to recruit Medicare beneficiaries. As Anointed's Assistant Director of Nursing, he falsified medical records to support Anointed's fraudulent claims to Medicare for services that were medically unnecessary and never provided.

The Dangers of EHR Documentation

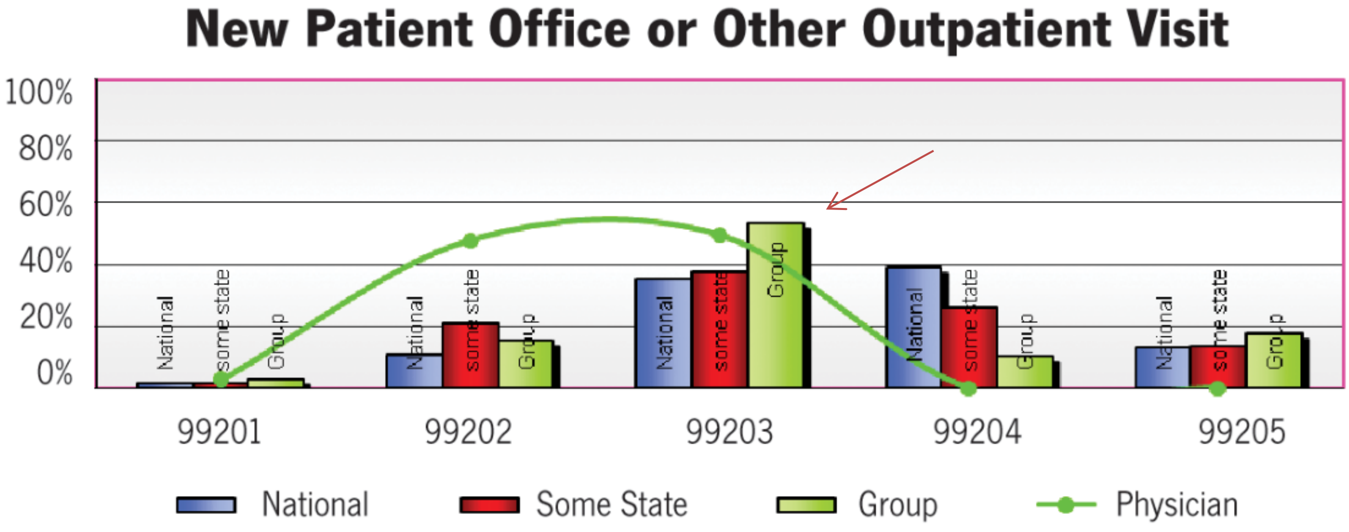
The Dangers of Electronic Health Record Documentation seems to be an appropriate topic to review with the recent implementation of this new single instance of EPIC. Our entire practice is focused on developing the skills needed to navigate the system and use the new features. Hopefully, we will quickly master this system which will make all of our jobs easier and more efficient.

One of the wonders of the electronic medical record is the auto charge capture feature. The software attempts to guide you to capture the correct charge for the services that you have provided. The main problem that arises from this auto guidance is, it is only as good as the information entered into the system. When choosing the correct evaluation and management (E&M) CPT code, medical necessity carries more weight than any other area of the service. As amazing as the system is, it cannot think thru medical necessity. You must be sure that you are documenting what is necessary to treat your patient. Also, you must be sure that you are not "over documenting" which may cause you to choose a higher level code then medically necessary. Would another provider treating this patient for the same issue, do the same thing?

Evaluation and management (E/M) codes are the most troublesome as well as the most audited codes.
Upcoding is a problem, but downcoding is also a big risk.

In 2017, the OIG (Office of the Inspector General) noted that 42% of E/M claims were incorrectly coded!! Medicare reported a 65-70% error rate for codes 99215, 99223 and 99233 (high level codes). That's HUGE!!

High level service codes are naturally flagged when a provider is identified by the number of high level service codes that fall outside the bell curve of other providers in his/her specialty in the same area of the country. These providers are labeled "Outliers"



Documentation that supports the medical necessity of the correct level of service is what we must strive to achieve.

Some points to remember: History of present illness, or HPI, is the only part of the history and exam that cannot be auto filled by the EHR. It is very important to document four clear elements (what, where, when, how, why and modifying factors) of the history of present illness.

You must state if this is a new condition or if you are seeing the patient for a follow up to an ongoing issue. If you are seeing the patient for follow up. You must say what you are following up on. Each note stands alone. The federal or contract auditors will only receive this specific note when requesting documentation. They do not receive the entire chart. All of the documentation needed to support the code must be in this specific note.

You cannot code or count conditions that you do not address in your documentation. If you are seeing the patient for a painful knee, are you really factoring in the patient's history of stable high blood pressure? If so, document what you are concerned about and how you are addressing it. Then, and only then, you can count it or factor it into your level of care. Also, you cannot count associated signs and symptoms as separate issues. For instance, if you are seeing a patient for a painful knee, you would not count "swollen knee" as a separate issue.

Department of Justice
Office of Public Affairs

Original date: Friday, April 6, 2018

Department of Justice and Health and Human Services Return $2.6 Billion in Taxpayer Savings From Efforts to Fight Healthcare Fraud

Departments Work to Stamp out Pill Mills and Opioid Overprescribing

The Department of Health and Human Services and the Department of Justice recently released a fiscal year (FY) 2017 Health Care Fraud and Abuse Control Program report showing that for every dollar the federal government spent on healthcare related fraud and abuse investigations in the last three years, the government recovered $4. Additionally, the report shows that the departments' FY 2017 Takedown event was the single largest healthcare fraud enforcement operation in history.

In FY 2017, the government's healthcare fraud prevention and enforcement efforts recovered $2.6 billion in taxpayer dollars from individuals and entities attempting to defraud the federal government and Medicare and Medicaid beneficiaries. Some of these fraudulent practices include:

- Providers operating "pill mills" out of their medical offices.
- Providers submitting false claims to Medicare for ambulance transportation services.
- Clinics submitting false claims to Medicare and Medicaid for physical and occupational therapy.
- Drug companies paying kickbacks to providers to prescribe their drugs, and pharmacies soliciting and receiving kickbacks from pharmaceutical companies for promoting their drugs.
- Companies misrepresenting capabilities of their electronic health record software to customers.

"Today's report highlights the success of HHS and DOJ's joint fraud-fighting efforts," said HHS Secretary Azar. "By holding individuals and entities accountable for defrauding our federal health programs, we are protecting the programs' beneficiaries, safeguarding billions in taxpayer dollars, and, in the case of pill mills, helping stem the tide of our nation's opioid epidemic."

The Departments of Justice (DOJ) and Health and Human Services (HHS), through the Health Care Fraud Prevention and Enforcement Action Team (HEAT) effort, use data analytics and surveillance to crack down on, prevent and prosecute healthcare fraud. With teams comprised of law enforcement agents, prosecutors, attorneys, auditors, evaluators and other staff, last year DOJ opened 967 new criminal healthcare fraud investigations of which federal prosecutors filed criminal charges in nearly half of them.

Beyond criminal prosecution, in FY17 the HHS Office of Inspector General (OIG) excluded 3,244 individuals and entities from future participation in in federal health programs. HHS can also suspend Medicare payments to providers during investigations of credible allegations of fraud. During FY 2017, there were 551 related payment suspensions.

More than 4 million claims are reviewed by Medicare each day; resulting in more than one billion claims processed annually for timely payments to healthcare providers and suppliers. Given the volume of claims processed by Medicare each day and the significant cost associated with conducting medical review of an individual claim, the Centers for Medicare and Medicaid Services uses automated edits to help prevent improper payments without the need for manual intervention. The National Correct Coding Initiative consists of edits designed to reduce improper payments in Medicare Part B, and this program saved Medicare $186.9 million during the first nine months of FY 2017.

Last July, DOJ and HHS announced the largest ever healthcare fraud enforcement action, involving 412 charged defendants across 41 federal districts, including 115 doctors, nurses and other licensed medical professionals, for their alleged participation in healthcare schemes involving approximately $1.3 billion in false billings. Of those charged, more than 120 defendants, including doctors, were charged for their roles in prescribing and distributing opioids and other dangerous narcotics.