SAINT LOUIS UNIVERSITY

OFFICE OF UNIVERSITY COMPLIANCE

Dangers of Down-coding

Many times during coding and documentation reviews it is assumed that the focus is to determine whether or not a provider is up-coding to receive higher payments than that they would receive for the services that were actually performed. Up-coding can take many forms including charging a higher level evaluation and management (E/M) code, unbundling surgical procedures inappropriately, or coding diagnoses that are not supported in the medical record. Chapter 1: General Correct Coding Principles of the National Correct Coding Initiative's (NCCI) policy manual states in addition to up-coding "Physicians must avoid down-coding. If a code exists that describes the services performed, the physician must report this code rather than report a less comprehensive code…" It is not uncommon to find providers down-coding their services in attempt to fall under the radar of internal and external auditors. However, doing so could potentially backfire by skewing the provider's utilization data and presenting them as an outlier (Verhovshek). This will ultimately put them at risk for the very thing the providers are trying to avoid.

In addition to the risks for audits, down-coding services and diagnoses has the potential to harm patients as well as providers in a variety of ways. For example, an under-coded diagnosis will not accurately portray the patient's condition to their insurance company. This may affect their future coverage for required treatments. In cases where payers require Hierarchical Condition Category (HCC) coding, the under-reporting of diagnoses for a particular patient could result in lower payment rates to the provider. Similarly, under-coding evaluation and management (E/M) and other procedural services will also lower the revenue received and misrepresents the services performed during that encounter.

The Centers for Medicare & Medicaid Services (CMS) 2015 Comprehensive Error Rate Testing (CERT) reported that providers left more than $1 billion of on the table because of down-coding of claims. These services include E/M service, coronary artery bypasses, nursing home visits, subsequent hospital visit, and major joint replacements (Dooley). With these recent findings it is safe to assume that CMS and other payers will be keeping a keen eye out for those physician outliers to ensure that proper coding practices are taking place.

It is recommended by many that periodic internal audits take place to ensure that providers are aware of their current billing trends. Along with the individual department's billing review prior to billing, the Compliance Department performs a retrospective review annually on every billing provider to ensure accuracy in their billing, coding and documentation. Aside from any feedback sessions post review, we welcome providers to contact us at any time should they have billing, coding, or documentation questions.

Dooley, S. (2016, February 12). CMS's 2015 CERT Report Reveals Dangers of Upcoding and Downcoding. Retrieved June 15, 2016, from http://blog.supercoder.com/compliance/cmss-2015-cert-report-reveals-dangers-of-upcoding-and-downcoding/

Verhovshek, G. J., MA, CPC. (2016, February 03). Upcoding vs. Downcoding: Know the Difference. Retrieved January 15, 2016, from http://www.physicianspractice.com/coding/upcoding-vs-downcoding-know-difference

Requirements for International Travel

Information Security and Compliance have created new requirements for international travel with University laptops. Any staff or faculty member wishing to access network applications or files on the Saint Louis University shared drives will need to do so through a Virtual Private Network (VPN) or Authentic8 software, dependent on the country of destination. The following National Security level countries will require Authentic8 software for access to web based SLU applications and files : **Albania, Armenia, Azerbaijan, Belarus, Cambodia, China, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam**. Please contact the Service Desk at 977-4000 or Neil Smarko, nsmarko@slu.edu,for information on loading Authentic8 onto your machine.

All other international travel will require the use of a VPN for access to network applications or information on SLU shared drives. ITS Service Desk will be able to assist you with setting up the VPN to work with your machine during your international travel.

Information Security has purchased additional "clean" laptops available for loan to travelers. A "clean" laptop has a new image installed after each international trip, ensuring the elimination of viruses and malware. These machines are highly recommended for the countries listed in bold above. These machines are available on a first come basis; please contact the Service Desk for additional information 977-4000.

If you are traveling internationally, please contact the Export Control Officer to ensure the University remains in compliance with all federal Export Control regulations. Michael Reeves, mreeves8@slu.edu, 977-5880.

Cindy's Coding Corner

Documenting and Reporting Obesity/Morbid Obesity/BMI for Adults

According to the Centers for Disease Control & Prevention, overweight and obesity are both labels for ranges of weight that are greater than what is generally considered healthy for a given height. The terms also identify ranges of weight that have been shown to increase the likelihood of certain diseases and other health problems.
The following are tips for documenting and reporting obesity/morbid obesity and body mass index (adult):

- Document any current symptoms and physical exam findings related to obesity, morbid obesity, overweight, etc.
- In the final Assessment, document the overweight or obesity diagnosis to the highest level of specificity.
- Document any co-existing diagnoses that are impacted by the overweight or obesity diagnosis
- Document any specific treatment plan for the obesity diagnosis (e.g. referral to nutritionist; education; etc.)

If a patient's height and weight are noted within the medical chart, a coder/biller should not assume and calculate the BMI themselves to report in the claim. The BMI Z code should only be reported if the provider documented the specific BMI in the medical or clinical record, and the associated significance of the BMI to the patient's obesity, in relationship to current conditions and disease processes.

Additionally, ICD-10-CM Official Guidelines for Coding and Reporting 2016 offers guidance for "Documentation for BMI, Non-pressure ulcers, and Pressure Ulcer Stages" (Section I.B.14): "For the Body Mass Index (BMI), depth of non-pressure chronic ulcers and pressure ulcer stage codes, code assignment may be based on medical record documentation from clinicians who are not the patient's provider (i.e. physician or other qualified healthcare practitioner legally accountable for establishing the patient's diagnosis), since this information is typically documented by other clinicians involved in the care of the patient (e.g. a dietician often documents the BMI and nurses often documents the pressure ulcer stages). However, the associated diagnosis (such as overweight, obesity, or pressure ulcer) must be documented by the patient's provider. If there is conflicting medical record documentation, either from the same clinician or different clinicians, the patient's attending provider should be queried for clarification.

The BMI codes should only be reported as secondary diagnoses. As with all other secondary diagnosis codes, the BMI coders should only be assigned when they meet the definition of a reportable diagnosis (see Section III, Reporting Additional Diagnoses)."

SLU Launches New Secure Research Environment

Saint Louis University recently implemented a secure environment for research with sensitive data (social security numbers, electronic health records, etc.). This is an important milestone for SLU's research community in light of the increasing federal regulations for security and data protection in research.

This virtual FISMA-compliant computing environment and infrastructure will enable researchers to apply and effectively compete for grants and contracts requiring support for and adherence to the Federal Information Security Management Act (FISMA). The environment provides highly-secured computing-servers, database instances, and data storage, and ensures the protection of highly-sensitive research data created, used, or stored by the University's research departments.

The Federal Information Security Management Act of 2002 (FISMA) requires a minimum set of security controls and protection of the sensitive data created, stored, or accessed by either the federal government or any entity on behalf of the federal government. Certain federal organizations - such as the National Science Foundation (NSF) or the National Institutes of Health (NIH) - might require researchers to abide by these FISMA regulations in their contracts and grants. Compliance with FISMA is mandatory when the grant requires the research organization to return the data to the federal project sponsor, or if the grant has been awarded using a contracting form. SLU's ability to provide a secure environment for the research community to meet these requirements will provide an edge for SLU researchers when competing for these and similar grants.

For questions about the secure research environment, please visit the Research Technology Group's website or contact your grant administrators or the Research Technology Group at rtg@slu.edu. For more information on FISMA, please visit https://www.dhs.gov/fisma.

Contact Us

Elizabeth Cooley
Director
cooleyea@slu.edu
977-5774

Kerry Borawski
Asst. Director
Research Compliance
kborawsk@slu.edu
977-7720

Ron Rawson
Privacy Officer
rawsonr@slu.edu
977-5884

Michael Reeves
Export Controls Officer
mreeves8@slu.edu
977-5880

Theresa Brewer
Compliance Coordinator
tbrewer3@slu.edu
977-5889

Hannah Halstead, MSW
Research Auditor
halstehf@slu.edu
977-5887

Anne Schwartze, RHIA, CPC
Physician Billing Auditor
aschwa22@slu.edu
977-5885

Mickey Coriell, CPMA
Physician Billing Auditor
coriellm@slu.edu
977-5886

Janet Flach
Executive Assistant
Jflach1@slu.edu
977-5772

Location:
Schwitalla Hall, M229

Main Number:
977-5545

Fax Number:
977-5195