SAINT LOUIS UNIVERSITY

OFFICE OF UNIVERSITY COMPLIANCE

Compliance E-Newsletter April 2016

Welcome Mickey Coriell!

The Office of University Compliance would like to welcome Michelle "Mickey" Coriell to the physician billing audit team**.** Mickey started her career at SLU in 1993 as a Patient Care Technician. She transferred to the Department of Anesthesia in 2000 and earned her CPC credentials in 2005. Mickey left the University for a short time in 2008, but continued billing for another academic facility. She returned to the Department of Anesthesia in 2010 and earned her Certified Professional Medical Auditor (CPMA) in 2015.

Outside of work Mickey enjoys coming home to her husband Tom and their three dogs. She loves spending time with her children and ten grandchildren. In her free time, Mickey and her husband enjoy "clowning around." Mickey (a face painter) and Tom (a Shriners Clown) volunteer to help raise money for the Shriners Hospital.

Information Security Changes 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.

SAINT LOUIS UNIVERSITY
COMPLIANCE
877-525-KNOW

PROTECTING DATA USED IN RESEARCH

Saint Louis University has a duty to protect the confidentiality and integrity of sensitive and confidential information as required by law and professional ethics.

Individually identifiable health information used in research is considered sensitive and must be safeguarded in compliance with HIPAA regulations. Investigators and individuals responsible for the release, storage, or transfer of research data, must ensure that it is kept in accordance with SLU information security policies and supporting standards.

Minimum Necessary

Data should be kept in a manner that minimizes risk to research participants. This can be accomplished by applying the minimum necessary rule.

- Collecting/storing the minimum amount of identifiers as necessary
- Giving access to the minimum amount of persons as necessary
- Restricting data to the minimum amount of sensitive information necessary

De-Identification

When designing new research protocols, investigators should take into consideration the type of data they will create in the study and put the appropriate data protections in place. Risk elevates as data is more sensitive, more identifiable, and/or when data is shared with greater numbers of individuals or externally. There are options to limit the identifiability of data.

- Collect the data in an anonymous fashion
- De-identify the data collected for research
- Use coded datasets and maintain master lists separately

Do NOT store identifiable research data on personally owned laptops or flash drives.

Appropriate safeguarding is a requirement at all times when using identifiable health information in research.

- Only share data with authorized individuals (those identified in IRB approved protocol)
- Store data on University approved applications or locations (i.e. REDCap)
- Use encryption for storing research datasets
- Hard copy data must be secured from unauthorized access and properly destroyed when appropriate.

Access to research data, whether electronic or hard copy, is ultimately the responsibility of the Principal Investigator.

Investigators are expected to follow the data management plan detailed in the approved IRB protocol. Any deviations from the plan must be approved by the IRB via submission of an Amendment prior to implementing the change; failure to do so could put study participants at risk and will be considered a protocol violation that is reportable to the IRB.

Questions contact: Ron Rawson, Privacy Officer at 977-5884 or IRB at irb@slu.edu

Sunshine Act Update

The Centers for Medicare and Medicaid Services Open Payments portal is available for review by physicians through **May 15, 2016**. CMS will publish the 2015 payment data and updates to the 2013 and 2014 data on June 30, 2016. In order for any disputes to be addressed before the June 30th publication, physicians and teaching hospitals must initiate their disputes during this review period, and industry must resolve the dispute before the publication deadline. Review and dispute is voluntary, but strongly encouraged by CMS. The University is not allowed a role within the Open Payment System, and therefore cannot review the data prior to publication on the physician's behalf.

Registration instructions published by CMS can be found at https://www.cms.gov/OpenPayments/Downloads/Quick-Reference-Guide-Enterprise-Identity-Management-System-Registration.pdf

CINDY'S CODING CORNER

ICD-10-CM: Hypertensive Chronic Kidney Disease

A causal relationship between hypertension and chronic kidney disease is **always presumed** and documentation of hypertension with chronic kidney disease is always reported as hypertensive chronic kidney disease. (ICD-10-CM Coding Guidelines Section I.C.9.a.2)

- A code from category I12, Hypertensive chronic kidney disease, is assigned first when there is documented hypertension and a condition classifiable to category N18, Chronic kidney disease (CKD). A code from category N18 is reported secondarily to identify the stage of chronic kidney disease.
- If the patient has hypertensive chronic kidney disease and acute renal failure, an additional code for the acute renal failure is also assigned.

Kerry Borawski
Interim Director
kborawsk@slu.edu
977-7720

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

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

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

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

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

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

Cynthia Stacy,CPC, CPMA, CPC-I, CRC
Compliance Education Manager
stacyc@slu.edu
977-5888