SAINT LOUIS UNIVERSITY
COMPLIANCE
877-525-KNOW

May 2015

MID-LEVEL PROVIDERS: *WHAT YOU NEED TO KNOW*

The Office of University Compliance, accompanied by SLU*Care* Administration and the Practice Management Operations (PMO), will be hosting a training session, “Mid-Level Providers: *What You Need to Know*.”

This education initiative will assist the mid-level providers in achieving the highest standards in business practices for SLU*Care.* This two hour seminar will focus on Mid-Level Providers’ clinical care, Missouri regulations, documentation and billing, and the physicians’ role when working with Mid-Level Providers.

Guest Speakers:

Lyn Chew, RN, MBA, LNHA, CPC, CPC-H, CHC
Principal, Compliance Concepts, Inc.
Lyn is experienced in facility operations and management advisory services for practitioners, research, and the long-term care industry. She specializes in the provision of compliance training and education and the performance of billing, coding and documentation reviews. She is a certified professional coder (CPC), certified professional coder-Hospital (CPC-H) and a licensed nursing home administrator (LNHA).

Richard D. Watters, Lashly & Baer, P.C.
Richard advises all types of health care clients from large hospital systems to individual physicians, nurses and other health care professionals on various matters including general health care laws and regulations, business operations, physician contracting, governance and corporate issues, licensing/regulatory compliance, the Stark Law, fraud and abuse, EMTALA, Certificates of Need, medical staff issues, practice and business acquisitions, joint ventures, Medicare and Medicaid conditions of participation, and reimbursement and contract negotiations. Mr. Watters has been selected by his peers for inclusion in *The Best Lawyers in America*® in the field of Health Care Law for the last 20 years, and in 2011 he was elected the Lawyer of the Year for St. Louis by *The Best Lawyers in America*®.

Times and Locations:

Chairs, Physicians, and Mid-Level Providers: The following sessions will focus on clinical care from mid-level providers, documentation, as well as the providers’ role when working with mid-level providers. (All of these sessions provide the same information.)

DATE	TIME	LOCATION
Tuesday, May 19, 2015	12:00 pm – 2:00 pm	LRC PITLYK Auditorium B
Tuesday, May 19, 2015	5:00 pm- 7:00 pm	LRC PITLYK Auditorium B
Wednesday, May 20, 2015	7:00 am- 9:00 am	Schwitalla Hall Lecture Hall 3

REGISTER HERE

Business Managers, Directors, Billing Supervisors, and Billers: The following sessions will focus on billing and documentation for services provided by Mid-Level Providers and their collaborating physicians: (All of these sessions provide the same information.)

DATE	TIME	LOCATION
Tuesday, May 19, 2015	9:00 am- 11:00 am	LRC PITLYK Auditorium B
Thursday, May 21, 2015	8:30 am- 10:30 am	LRC Auditorium C

REGISTER HERE

Who's in the Dog House?

Anthem Breach Sounds Alarm

Anthem, the second largest health insurer in the United States, suffered a major data breach. Over 80 million current and former customers had their names, medical IDs/social security numbers, street addresses, and employment information stolen. The database hacking incident makes it clear that the healthcare sector is a target for hackers.

The healthcare industry is anxiously awaiting more details about the nature of this attack. A senior White House official and lawmakers are saying the incident is part of a disturbing trend of massive data breaches impacting consumers' information.

When details of the Anthem breach are confirmed, it's highly likely the incident will rank as the largest health data breach since enforcement of the HIPAA breach notification rule began in September 2009.

A spokeswoman for the Department of Health and Human Services' Office for Civil Rights, which oversees HIPAA enforcement, confirmed that the incident would qualify as a breach under HIPAA, based on the type of information the company says was exposed.

Under HIPAA, fines range from $100 to $50,000 per violation. The level of the fine depends on whether the entity knew of the security gap, acted on the gap, or even whether the decision to not address the gap was a willful decision. There are fine caps for each statutory violation. Assuming OCR finds that 1) Anthem failed to safeguard the data and 2) there was an impermissible use or disclosure, the statutory fines would cap out at $1.5million for each violation, for a total of $3million.

While, this fine represents the maximum amount that could be levied as a statutory penalty, it does not include costs of credit monitoring and notification. Add to this, the class action law suits for negligence, state mandated penalties/fines, and Anthem has a very serious problem.

Rep. Lynn Westmoreland, R-Ga., Chairman of the Intelligence Committee's NSA and Cybersecurity Subcommittee, said: "The Anthem hack shows the immediate need for enhanced cybersecurity measures, for both national security purposes and to protect our citizens. The hackers have exposed the weaknesses in our current system, and have jeopardized sensitive and personal data.

Any organization that holds sensitive data is at risk. That is why it is so important that organizations conduct a careful review of their risk analysis and risk management plans to ensure that appropriate safeguards are in place to address the threats and vulnerabilities to individuals' data.

TIPS FOR TRAVELING WITH TECHNOLOGY

Many people will be traveling this summer, the majority traveling with technology. Here are a few helpful tips to assist in safely using your devices:

- ✓ Secure your laptop or other mobile device with a strong password, OS Security Updates, anti-virus, anti-spyware and firewall software.
- ✓ Before you travel, back up your files.
- ✓ Do not connect to any unsecured Wi-Fi hotspots; you should only be accessing University/Sensitive Data via VPN.
- ✓ If you are travelling internationally, contact the University Export Control Officer, Michael Reeves, 977-5880, mreeves8@slu.edu to ensure compliance with federal regulations.
- ✓ If you have additional questions about securing devices, contact infosecurityteam@slu.edu
- ✓ If an incident occurs while travelling, immediately contact infosecurityteam@slu.edu