SAINT LOUIS UNIVERSITY
COMPLIANCE
877-525-KNOW

October 2013

Breach Prevention: *Critical for Compliance*

What is a Data Breach?

Key Definitions

Protected Health Information (PHI): is individually identifiable health information that is transmitted or maintained in any form or medium by a health care provider, health plan, or health care clearinghouse.

Personal Information: is an individual's first name or first initial and last name, in combination with any one or more of the following: social security number; driver's license number; or financial account number, credit or debit card number, in combination with any required security code, access code or password.

Breach of PHI: A breach of protected health information (PHI) is defined by federal law and regulation to mean the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule of HIPAA which poses a significant risk of financial, reputational, or other harm to the individual.

Breach of Personal Information: Missouri Statute defines "breach of security" or "breach" as unauthorized access to and unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information.

Prevent Data Breach

WHAT SHOULD I DO?

A recent study by PricewaterhouseCoopers found that only 5% of data breaches are caused by malicious cyber-attacks, almost 55% are linked to human error, and 44% are due to third-party handling of data.

Tips for Preventing a Breach

- Destroy unnecessary patient information – shred documents, delete electronic files
- Verify the number and recipient of a fax before sending
- Limit the printing of PHI or Personal Information
- Verify that all pages of printed documents belong to the patient or intended recipient before presenting
- Limit the use of email containing PHI or Personal Information
- Verify the recipient's address before sending an email
- NEVER use email for transmitting PHI outside of SLU unless encrypted
- Do NOT store patient information on portable devices unless encrypted
- Log-off or secure your computer when away from your workstation
- Lock laptop computers and other portable devices in secure location when not in use

Federal and State laws and regulations define breach notification requirements associated with unauthorized use or disclosure of Protected Health Information (PHI) or Personal Information. Each event that involves breach of individually identifiable PHI or Personal Information must be evaluated for application of the applicable regulatory notification requirements.

Know or Suspect a Breach Incident

WHAT SHOULD I DO?

If you know of or suspect a breach of protected health information (PHI) or personal information, it is your obligation to report the incident to the Privacy Officer, Ron Rawson, or your supervisor for reporting to the Compliance Office. (977-5545)

The Privacy Officer will initiate a follow-up investigation with appropriate management to document and review details of the incident. Assessment of the incident will result in recommendations to mitigate harm along with actions specific to the applicable breach notification and reporting requirements.

Spooktacular Compliance Education Sessions:

General HIPAA Session
November 14, 2013
3:00 – 4:00 pm
Learning Resource Center
Room 110

Billers Meeting
The "In" Crowd:
Auditing and Coding Inpatient Services
November 19, 2013
10:00am to 11:30pm
LRC 112-113
1.5 CEU-AAPC

Coding Clinic
Inpatient Documentation, Coding, and Charge Capture

November 5, 2013
12:00 pm
7th Floor Hanlon Conf. Room
SLU Hospital, Bordley Tower

November 21, 2013
5:00 pm
8th Floor Fitch Conference Room
SLU Hospital, Bordley Tower

Research Compliance

The NIH Office of Inspector General reports that the University of Colorado-Denver charged at least $1.2 million in unallowable expenses on their HHS awards in FY2010. The NIH blames inadequate institutional oversight; "… the University largely left it to the discretion of its individual colleges, departments, and principal investigators to interpret the University's policies and procedures for charging costs to Federal awards correctly and to comply with Federal regulations and guidance."

Decentralizing research compliance responsibilities requires (1) Training, (2) Communication, (3) Monitoring and (4) Feedback. The Research Division at Saint Louis University hosts a variety of training sessions which include Allowable Costs, Effort Reporting and monthly Business Manager meetings. They promote communication and provide feedback through the relationships established by Grant Accountants and Grant Development Specialists with individual researchers. Finally the Office of Sponsored Programs provides detailed monitoring of all expense transactions. http://oig.hhs.gov/oas/reports/region7/71106013.asp 6/7/2013 OIG Audit Report

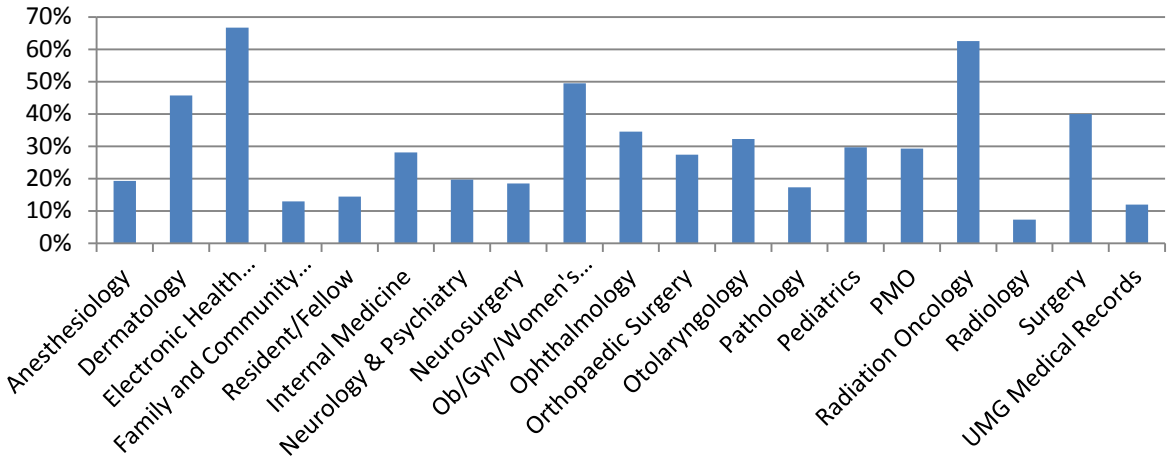
LESS THAN 30 DAYS REMAIN

to complete the

Mandatory Annual Compliance Update!!!

The Compliance team has randomly selected two employees to receive special "Completed Prize" for completing the Annual Compliance update. Congratulations to MaryLynn Mueller from Otolaryngology and Adrienne Smith from Surgery. Your prize will be delivered soon!! Each week we will draw two more winning names until the November 15th. To see the completion percentage rate of your department see graph below.

Annual Compliance Update % Complete



67% of the EHR Team have completed the Annual Compliance Update