SAINT LOUIS UNIVERSITY
COMPLIANCE
877-525-KNOW

May 2014

How Do I Keep Data Safe?

The Responsible Conduct of Research program has many compliance training requirements, including face-to-face training. Nick Lewis, Information Security Officer and Director of IT Security and Compliance in ITS, recently hosted a 2-hour presentation to a group of researchers titled "How Do I Keep Data Safe?" In this presentation, many questions emerged around a variety of subjects. Hot topics were transmitting data securely through encryption, mobile device security and cloud use for sensitive data. Let's tackle encryption in this article.

First things first, let's define sensitive data. Sensitive data is a blanket term used to designate classes of data with a high level of sensitivity that the University is legally or contractually required to protect. At Saint Louis University, sensitive data refers to:

- ✓ ***Restricted data*** is University-maintained, electronically stored data for which inappropriate use or access presents a high to very high reputational and/or business risk to the University. Restricted data typically is subject to significant legal requirements for the protection of the data and includes data/information such as social security numbers, medical records, information related to students, human resources, donors or prospective donors, financial data, contracts, credit card numbers, research and clinical human subject or government contract data and certain classified management information.
- ✓ ***Confidential data*** is University-maintained, electronically stored data for which inappropriate use or access presents a medium to high reputational and/or business risk to the University. Confidential data is typically subject to legal requirements for University protection of the data arising under contractual non-disclosure obligations and includes a subset of restricted business units, colleges, schools or departmental data.

Transmitting Data Securely

When we talk about secure data transmission, encryption is one method end users can use to help ensure that the confidentiality of their sensitive data is maintained. Here are some of the FAQs regarding encryption:

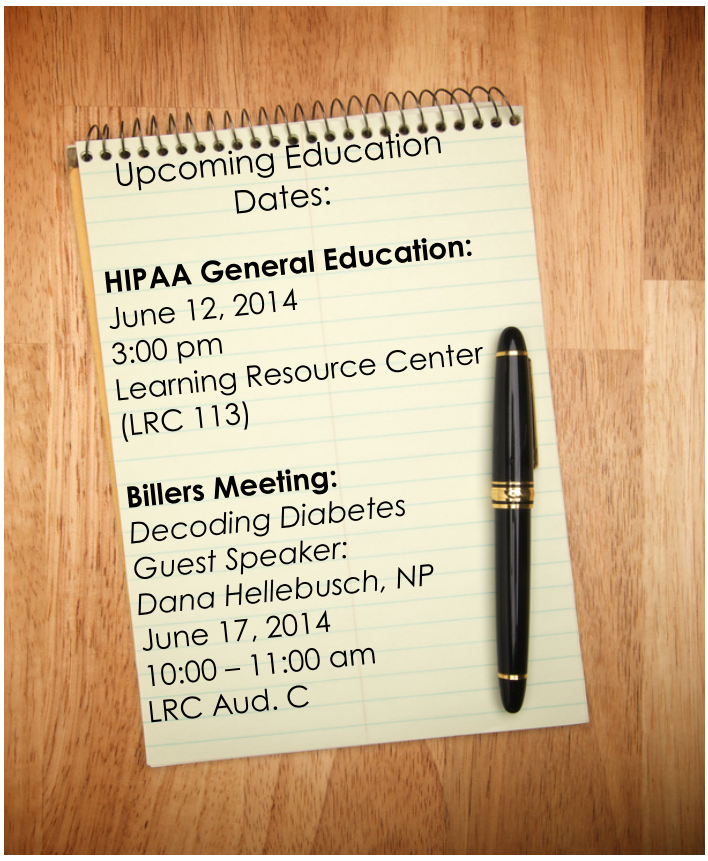
1) *What is encryption?* Encryption is a method of encoding information from a plain text format into unreadable text.
2) *Why is it important for us at SLU?* Many of us handle sensitive data or information that we need to share for various reasons. We need to make sure we are doing this securely, and encryption can help with that.
3) *If I email a document to a co-worker, is it encrypted?* If you email from a slu.edu to slu.edu mail account, by default it is encrypted when the email is going from one account to the other. But if you email outside of our network, it is no longer encrypted by default. For instance, if you forward a work email to your personal email account, it is not encrypted. Keep this in mind when collaborating with other universities or hospitals.
4) *What if I de-identify the data, do I need to encrypt it still?* No. If you remove all of the personally identifiable information (PII) from the document, you do not need to encrypt it.
5) *How can I encrypt documents?* There are many methods to consider. If you have Symantec Drive Encryption (full disk encryption), you can use Symantec PGP Zip that is included with the SDE license. However, this type of file cannot be emailed in our current system, so you will need to use Send This File (available via mySLU/Tools). If you do not have SDE, there are some additional options for document encryption:
    - Encrypting Documents in MS Office 2007, 2010 (link to page)
    - Encrypting Documents in Adobe Acrobat Pro 9 (link to page)
    - Encrypting Documents in Adobe Acrobat Pro 10 (link to page)
6) *What else do I need to know about encryption?* **ITS cannot help you recover passwords for documents you encrypt,** so here are a few important guidelines before you encrypt:
    - Have a backup of the document - Keep a backup of the document on your U drive (or network storage). If you lose the password, it is not recoverable so the information will be lost.
    - Store your passwords in a safe place - Each document will require a password so this could amount to managing many passwords. Using an application that manages passwords is recommended.
    - Communicate the password for the document wisely - Sending the password in the same email as the encrypted document is not a good practice. Communicating the password via telephone or voice mail is a much more secure way to communicate the password. The recipient can also try to open the file while you are one the phone to verify that they can open the file.

For more information about our full disk encryption program and document encryption, see our webpage slu.edu/infosecurity.

Tips for Traveling with Technology

Many people will be traveling for Summer vacation, 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



Please feel free to contact the Office of University Compliance at (314) 977-5545 or at slucompliance@slu.edu

■■■

If you need to reference past newsletters, upcoming education dates or need more information on Compliance visit our website.