



SAINT LOUIS UNIVERSITY COMPLIANCE 877-525-KNOW

JULY/AUGUST
2015



Upcoming Education Dates:

Billers Meeting:
September 22, 2015
10:00 – 11:00 am
LRC Room 112



Feel free to contact the Office
of University Compliance at
(314) 977-5545

...
*If you need to reference past
newsletters, upcoming
education dates or need more
information on Compliance, visit
our [website](#).*

Encryption of University Laptops

Data breaches have become a common news item. They usually involve sensitive information that potentially impacts hundreds or thousands of consumers. One common source of data breaches is lost or stolen laptops. If you travel with your computer or keep it in a place where other people can put their hands on it, you're vulnerable.

While there is no single solution for preventing breaches, encryption is a reasonable and appropriate solution for securing mobile devices. Saint Louis University is implementing full disk encryption across campus. The software, Symantec Drive Encryption (also known as PGP) is being pushed to computers with assistance from department IT staff for all University managed Windows 7 laptops that access or store sensitive data.

The use of encryption on laptops will provide an additional level of protection for patient, staff, and student information. It will help prevent unauthorized access to data on the SLU network or individual hard drives and also shield the University from costly reporting requirements and fines.

How Do I Know If My Laptop Is Encrypted?

When logging into a University encrypted laptop you will first see the 'Appropriate Use' screen. The next screen is called the 'pre-boot' screen. You will need to enter your SLU User ID and password to allow access to your encrypted computer and continue the Windows log-in.

If you do not see the following screens when logging in to your laptop, it is not encrypted with the University's Symantec whole disk encryption software.

If your Windows 7 laptop has not yet been encrypted contact your department IT staff or the ITS Service Desk at 977-4000.

SAINT LOUIS UNIVERSITY

SLU Legal Notice for Computing Resources!

You are logging on to Saint Louis University's computing environment, which is governed by the University's Appropriate Use Policy and Information Security Policies. By Pressing Any Key to Continue, you are agreeing to follow this policy and all related Information Technology Security Policies. To familiarize yourself with these policies follow this link <http://www.slu.edu/info/policies-and-procedures/information-technology-policies>. Failure to comply with University information system policies may result in corrective action for individuals or departments involved. Questions or concerns may be directed to the ITS Service Desk at 314-977-4000.

Press Any Key to Continue!

SAINT LOUIS UNIVERSITY

User name:

Passphrase:

Domain: SLU

Use TAB key to move between fields. Use SLU Net ID & password to sign on!

Press F1 for Help. Press F4 for Forgot Passphrase.
Passphrase@SLU Password | Help at [www.slu.edu/its/information-security/symantec-drive-encryption-\(pgp\)](http://www.slu.edu/its/information-security/symantec-drive-encryption-(pgp))

Clinical Trials

Research Participant Payments

There are many regulations pertaining to payments made by the Research Team to participants of research studies, including the influence payments represent to the participants, the tax burden they may carry, and the need for caution with subjects who are also Medicare Recipients. The Office of University Compliance encourages Research Teams to respond to these issues with a thorough documentation for the processes used by the team in calculating payment amounts, distributing payments to participants, and fiscal record-keeping.

The general purpose of participant payments is to manage the financial burden a subject may feel related to their participation in a research study, without exerting undue influence on the potential subject. The Office for Human Research Protections (OHRP) describes "undue influence" as "an offer of an excessive or inappropriate reward or other overture in order to obtain compliance," so that the potential subject would not choose participation against their best interest. Calculating the appropriate amount then is difficult, because the magic motivating amount will vary by individual research subject based upon their own unique perspective. A research subject with no other discernable income may experience 'undue influence' for a \$10 participant payment, while another subject in the same study wouldn't bother for a mere \$10. If the Research Team documents the rationale used in calculating the appropriate payment amounts to cover transportation and other costs, they will safeguard against questions that surface about influence, despite diverse subject populations.

The Research Team should remember that a tax burden will exist for participant payments in all studies that, in aggregate, exceed \$600 per year as the IRS identifies such award payments as personal income. It is the University's responsibility to issue an IRS Form 1099 to participants who receive qualifying amounts, which include all payments made to the research subject by cash, check or gift card. The IRB's Consent Template includes a reference to this reporting process, which requires the collection of subjects' names and social security numbers for all cases of research participant payments, despite the form in which that payment is delivered (i.e., cash, check or gift card).

In cases where a research study visit also includes routine/standard of care services, the research protocol *may* allow for billing to Medicare. The study's Medicare Coverage Analysis (MCA) will identify this distinction, as a pure research visit would not allow for any Medicare billing. The Office of Inspector General released guidance entitled "Offering Gifts and Other Inducements to [Medicare] Beneficiaries" which limits "inexpensive gifts" to under \$10 per instance and under \$50 in annual aggregate, and considers anything greater to be an undue influence to utilize Medicare. In documenting their rationale for utilizing consistent participant payments within a research study, the Research Team can clarify that that the payment is not considered a gift to incentivize study enrollment.

An excellent article that may be helpful to Research Teams curious about participant payments can be found in the March 2014 Journal of Clinical Research Best Practices, authored by David Vulcano and titled "Ten Subject Stipend Issues". Documenting the decisions made by the Research Team throughout the participant payment process, including the calculation, payment process, and financial reporting, will protect the study and the University from future scrutiny on this highly regulated area.

2015

Annual Compliance Update

On August 5, 2015, the Office of University Compliance launched the 2015 Annual Compliance Update. The update is mandatory for all faculty and staff who work with protected health information (PHI), in a clinical setting, medical billing and coding, and/or research.

This online education initiative provides an overview of the current healthcare compliance climate including the prevention and detection of fraud, waste and abuse, SLU's Compliance program, updated information regarding HIPAA and Information Security, General Research Processes, Conflicts of Interest, Export Controls, Contracting Basics, and Risk Management.

The 2015 Annual Compliance Update will take approximately one hour to complete. This includes watching 2 videos and answering a number of questions after each video. The update must be completed by October 31, 2015.

[Click here](#) for detailed instructions on how to view and complete the update.

ICD-10

Biller/Coder's ICD-10
Training
Completion
Update

Phase	Completion %
1	96%
2	91%
3	86%