Keeping Your Data Safe in a Mobile World

In today's world, computers are becoming smaller and more mobile. The smart phone is a great example. Many of us do not realize we are carrying around a mini computer. Think of the things that can be done or stored on a smart phone. Do you text, store pictures, handle work and personal emails, or keep a contact list of work colleagues and clients on your phone? In addition to smart phones, many people routinely carry flash drives with important data, laptops for work, or now, the ever popular iPad or other tablet computer.

All of these devices provide easy, instant access to information. While ease of use and availability of information can make your time more productive, you need to remember if it is easy for you to access; it is easy for someone else to access as well. The University of Louisville must adhere to over 400 federal, state, and local regulations, many of which require safeguards for protecting sensitive information. Therefore, if University data stored on any of these devices is sensitive or falls under regulation, it needs to be protected. To ensure that sensitive information is protected, consider the following:

- Is the data *encrypted*? Most regulations and contracts require data covered under the regulation to be encrypted.
- Do you forward your University email to your phone? If you do, you need to make sure your phone is *encrypted*.
- Do you forward your email or store sensitive data on a flash drive, tablet computer, or laptop? If so, you need to make sure the data contained on the device is *encrypted*.
- Do you forward your work email to your personal email account? Do you store sensitive information in the cloud? If so, the data is going into an unprotected environment that would not be considered secure. Under HIPAA, FERPA, and PCI, this would constitute a breach of protected personal data.

The common safeguard noted in the above points is encryption. It is very important to make sure the data is protected to the fullest extent possible. Breaches of patient, student, or customer data occur on a daily basis. When the data is encrypted, it becomes inaccessible and a breach is avoided. If you think data breaches and compromises are irrelevant, consider the following…

Drug cartels are a $400 billion per year industry and headline the news. Did you know cyber-attacks and data breaches are over a $600 billion per year industry and only about 2% of the hackers ever get prosecuted? It is not a question *if* someone will try to access your data but *when*, so protect it.

Computer security is always too much, until it is not enough. A few preventive measures can save you from months of headaches if your sensitive information is breached. Please contact the University of Louisville's Information Security Office with any questions or concerns.