U-MIC TRANSCRIPT
Electronic Data Security

When collecting or storing confidential information electronically, you must take measures to guard it against unauthorized access. Internet hacking, theft, and lost computer equipment all present threats to the confidentiality of study data.

The Office of Human Research Compliance Review offers suggestions for securing personal and confidential electronic data. While the applicability of these suggestions depends on the nature of the study at hand, they reflect, in general, currently acknowledged *best practices* for electronic data security.

- Collect only the personally identifiable information you'll need to conduct your study. If you plan to de-identify your data, do so as soon as possible following data collection.
- Store identifying information separately from research data, and use encryption software to protect it from theft.
- Control who may access the machines you use to collect, store, process, or transmit identifying information, restricting access to members of your study team. Use only machines managed by IT professionals.
- Avoid storing identifying information on portable devices that are easily lost or stolen. If you need to store data on small devices, or transmit identifying information over the internet, make sure it is encrypted.
- Finally, securely delete all identifying information as soon as you no longer need it.

The University of Michigan's Information and Technology Services department offers suggestions for protecting the data you bring with you when you travel.

- Find out whether your IT department can lend you a machine to use while you travel. Bring only the machines and data that you'll need. Create a new, temporary password to use during your trip, and change it again as soon as you return.
- Create an inventory of the data stored on your machine, in case it is lost or stolen. Back up all data, and save the back-up on a machine that you will not bring on your trip. Full disk encryption helps to protect sensitive data stored on a lost or stolen machine.
- Many communities and businesses make wireless internet networks available to the general public. Avoid using these public networks on machines that contain confidential data. Instead, download and use the University's virtual private network (or VPN) client, which provides an encrypted network.
- Try to keep your machine with you at all times. If you do have to step away from your machine, use password-lock to prevent others from seeing your data.
- Contact local authorities if your machine is lost or stolen. Contact the ITS Service Center to help you change your passwords. If you believe that a lost or stolen device may have contained University-owned sensitive data, you must email security@umich.edu to make a report.

U-MIC TRANSCRIPT
Electronic Data Security

Contact your Information Technology department, and the Office of Human Research Compliance Review, for more information about electronic data security.

Posted: 6/12/2012