U-MIC TRANSCRIPT
Data Management and Security

The information technology community recommends eight minimum data security controls designed to protect the confidentiality of personally identifiable data about research subjects, as well as three additional controls for use when collecting and storing especially sensitive data. These recommendations represent a composite of suggestions and guidance pieces developed by several universities.

The eight minimum controls are as follows.

1. Password-protect all data collection and storage devices—such as computers—using a strong password. But, passwords in and of themselves are not considered sufficient for protecting data or information.
2. Therefore, all data and research files must be encrypted.
3. Keep identifiers, data, and codes in separate password-protected and encrypted files, and store each file in a different secure location.
4. When transmitting data electronically, use transport layer security—TLS, or sometimes SSL, for *secure sockets layer*—using a 128-bit encryption key.
5. Never store identifiers on laptop computers, PDAs, USB drives, or other portable devices. If you must use portable devices to collect identifiers, make sure the data files are encrypted and that you move the identifiers to a secure system as soon as possible. Lock any portable device in a secure location while it's not in use. Consult with your department's IT Security Liaison about correctly configuring desktop and laptop computers, as well as other external devices, in order to collect and store research data safely.
6. Whenever using email to communicate with subjects or to collect or transmit information about them, inform subjects that email is not secure. When transmitting research data via email, advise subjects to respond from email addresses to which only they have access.
7. Never transmit protected health information (or PHI) via email, except by qualifying email systems within the University of Michigan Health System and Medical School.
8. If you're using a remote data storage (or *cloud*) service, you must follow University guidelines at http://www.safecomputing.umich.edu/cloud and /google.

The IT community recommends three additional controls for use in research involving especially sensitive data. Higher-sensitivity data include PHI, personal identifying information, and other forms of sensitive information.

First, move all data from local devices to a secure UM server as soon as possible.

Second, implement password protection at multiple levels on each local device used for collecting and storing research data.

Third, delete or destroy identifiable information as soon as is practicable.

U-MIC TRANSCRIPT
Data Management and Security

Contact ITS or MSIS or see their websites for more information about research data management and security.

Posted: 5/15/2013