MICHIGAN LAW INFORMATION TECHNOLOGY UNIVERSITY OF MICHIGAN

Policy for Handling and Storing Sensitive Data for Law School Clinics

August 2020

To maintain the security of our institutional data, Law IT requests your compliance with the following policies:

Storage of Institutional Data

University policies govern how and where various types of institutional data may be stored. The Sensitive Data Guide to IT Services provides guidance by both data type and service. It also supplies a search tool for quickly looking up whether a particular type of data is permitted on a specific service.

The following additional policies apply to using Box:

- When storing and sharing sensitive data in U-M Box, use a Shared U-M Box Account that has been set up specifically for protecting sensitive data, and manage the sharing settings appropriately. See Using Box at U-M Securely with Sensitive Data
    - Law IT has set up a UMLS-designated folder for each clinic in accordance with the above policy. **Keep University and clinic data in the appropriate UMLS-designated folders on Box.**
- Never move University or clinic data to your own Box folders or personal Box account.
- University and clinic data should never be stored on your computer's hard drive or within its subfolders (including Documents and the Desktop.)
- Even though Law IT discourages it, if you need to store clinic data on an external storage device, you must purchase a special hardware encryption device.
- If you need additional or different types of storage, you must contact Law IT via a General InfoTech work request to make these arrangements.

Accessing Institutional Data

- Clinic employees and students are required to use two-factor authentication (Duo) for weblogin when accessing clinic data on Box.
- We suggest adding the UMLS-designated folders for your clinic on Box to your Favorites.
- Use only **U-M Box Core Apps**, such as **Box Drive**, **Box for Office**, or **Box Tools** for working with sensitive University data. **Do not store University data on Microsoft's cloud service or use the Box for Office Online integration to edit files containing sensitive data.**
- **Do not use Box Sync** to synchronize data between Box and your computer.

Reporting Requirements

Your use of the network is governed by the University's policies on computer use, which include strict, mandatory reporting requirements for infected or lost devices (*see infra* § III(g))

- Report any inappropriate use of clinic data to your clinic administrator.
- Report any possible loss of data to your clinic administrator and Law IT.

Additional Resources:

- Box at U-M Learning Resources

Laptop and Personal Device Security

Using a personal device for clinic work requires additional effort on your part to ensure the safety of the client sensitive data you are accessing. Several actions will improve the security of the data you handle:

- **Run anti-virus software**
  The University's recommended free anti-virus software for PCs is Windows Defender, and Sophos Anti-Virus for Home for Macs. There are numerous products on the market, just be sure to keep them up-to-date. Run a full scan of your system regularly to make sure nothing has been downloaded. For more information see: https://safecomputing.umich.edu/antivirus

- **Keep your device updated**
  For PCs, make sure Windows Update is turned on and manually check for new patches weekly. For Apple computers, click on Software Update in System Preferences at least weekly.

- **Use a host-based firewall**
  For PCs, you can activate and adjust your firewall by searching for "firewall" in the Start menu. Confirm that it is on. For Apple computers select System Preferences, Security & Privacy, then select the Firewall tab. Click the small lock in the lower left corner to unlock the settings. Select Turn On Firewall if it is not on already.

- **Secure your device**
  To secure your device, see the University's recommendations at: https://safecomputing.umich.edu/tools. You can further secure your device by registering it with the University's police at: https://police.umich.edu/?s=register_property

- **Encrypt the data you carry. Delete it as soon as you have finished your work and uploaded it to U-M Box**
  Encrypting the data on your computer can prevent unauthorized exposure of the data, should your computer be lost or stolen. If you use a PC you can use Microsoft's Bitlocker program to encrypt your entire disk. For details on using Bitlocker on a PC, see: https://technet.microsoft.com/en-us/library/c61f2a12-8ae6-4957-b031-97b4d762cf31.

  Macs can use FileVault. For details on using FileVault, see: https://support.apple.com/kb/ht4790

- **Learn more about sensitive regulated data and where it may be stored**
  To see what constitutes sensitive data, and where it may be stored according to University policy, see: https://www.safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data, and especially look at the new interactive guide to data storage at: https://safecomputing.umich.edu/dataguide/

- **What to do if you find malware on your system, or if you lose your device**
  Losing your laptop or having it become infected with malware, could create a situation the University defines as a serious security incident. Your handling of the situation determines how the University reacts to the incident. The types of incident to report include:
  - Unauthorized exposure of private personal information (which may lead to identity theft or misrepresentation)
  - Computer break-ins and other unauthorized use of U-M systems or data

- Equipment theft or loss

It is very important that you do as little as possible with your computer in the case of a virus. The more changes made to the system, the less that can be read forensically. Report the incident immediately and stay off your computer if at all possible. To report a laptop loss or virus, access a web browser from a different computer and go to: https://workrequest.law.umich.edu

- Select LawITSecurity, and enter a description of the incident. A Law IT security specialist will contact you as soon as possible. You may also contact any Law IT computer specialist to help you.
- To learn more about computer security at the University of Michigan, browse the web site https://safecomputing.umich.edu/