Guidelines for Sharing, Sending, and Storing Data

Keep Michigan Medicine data secure

Per the University Standard Practice Guide (SPG), sensitive data is defined as information whose unauthorized disclosure may have serious adverse effect on the University’s reputation, resources, services, or individuals. This includes protected health information (PHI), i.e. patient information.

Even if you think your work does not deal with sensitive data, your Michigan Medicine workstation has access to PHI sensitive information.

When you SHARE, SEND, or STORE files, it is advised to treat all like sensitive data.

- **To SHARE/TRANSFER** files with external parties, use MiShare.
  - Large files > 25 GB may be transferred; for details see this information on size limits.
- **To SEND FILES by EMAIL**
  - Email *within* Michigan Medicine, use your Outlook Exchange email.
  - Email *outside of* Michigan Medicine – including email to @umich.edu – is not encrypted or secure. To ensure that your message and attachments are encrypted, write [Secure] or [SECURE] in brackets in the subject line.
  - For more information: see the Michigan Medicine Knowledgebase page on Outlook
- **To STORE or BACK UP** files, use these options:
  - **M+Box** (unlimited data amount)
    - Please be aware that M+Box is not approved for sensitive data by default.
    - To use M+Box for PHI, be sure to refer to this section on the Safe Computing website detailing how to use M+Box for sensitive data.
  - **NAS** (network attached storage) = our internal network file share system
  - External flash drives to back up files – use these only if absolutely necessary. See this page for approved encrypted devices by Apricorn or Kingston.