Storage

- Avoid storage of identifiable and potentially confidential/sensitive data on mobile devices or unsanctioned cloud storage providers. See UM Data Classification policy for definitions of non-public data.
- For research studies, please follow the data management section of the study protocol once data collection is complete and/or prior to analysis.
- Especially relevant are requirements for retaining only de-identified data if specified, including removing identifiers as soon as feasible. Particularly sensitive identifiers include SSN, MRN, and health insurance policy numbers as well as email addresses and telephone numbers.
- Securely store data sets and restricting access to appropriate members of the research team, for e.g. one group may have access to a UM provided/controlled secure location where identifiable data is retained and another group can have access to the de-identified or coded data set.
- For portable devices such as laptops – either university supplied laptops or laptops that have University IT approved full disk encryption software installed should be used. Encryption can also be enabled for on-premises workstations. Consult the applicable IT group.
- An anti-malware application (e.g. Carbon Black, Microsoft Defender ATP) should be installed and updated regularly on all University workstations.
- Protected Health Information (PHI) should NOT be stored on mobile phones or tablets. Consult the appropriate IT group for current best practices and solutions for mobile devices, including approved apps e.g. EPIC Haiku and Canto.
- For mobile storage (USB Flash, hard drives) – avoid storing identifiable or confidential/sensitive data. If you absolutely must, then such devices MUST be encrypted. IT (at Medical 305-243-5999, https://miamiedu.sharepoint.com/sites/umedinsider-uhealth-it , help@med,miami.edu ; at Gables/RSMAS, 284-6565, help@miami.edu, https://www.it.miami.edu/) can provide assistance on encryption services for laptops, selection of appropriate mobile devices, secure remote access and other specific, current, secure practices.
- Physical controls (locked, file cabinet, card key restricted office area etc.) should be used for paper/printouts with identifiable or sensitive information.
- Paper/printouts with identifiable or sensitive information that need to be disposed of, should be shredded or placed in the approved University provided Shred-It bins (current vendor) for such information – NOT in the regular trash.
- Avoid use of sensitive or identifiable paper documents at home, including printing of such documents.
- If you have an unavoidable and approved use case i.e. explicit approval from your business unit leadership, then a plan/practice for proper disposal of such information is critical. Best practice is use of a crosscut shredder which is the preferred solution. At the very minimum, destroy all

areas with identifiable information such as name, address, telephone number, email address, MRN, institution/department/business unit or other identifiable information. Again, AVOID use unless absolutely needed. NEVER dispose of University documents with identifiable or confidential/sensitive information in the regular trash.

Cloud Storage

- If any information must be stored in the cloud, use ONLY University supplied Box or OneDrive accounts (accessible via your UM email address/SSO – NOT your personal Cloud accounts). Contact IT for additional information. Jackson residents should store Jackson solely related data on Jackson IT approved storage, including Jackson IT managed Sharepoint. Jackson residents should consult with Jackson IT/Compliance for current, appropriate practices.
- Be careful to only share with those involved in the project for the time period necessary to accomplish the purpose. Do not share any type of sensitive or non-public data out to "Everyone".
- Make sure individuals have the **minimum appropriate** user access (i.e., view only, cannot share/print/download, etc.) to accomplish the purpose. Here are some useful links:
    - Share OneDrive files and folders
    - Box FAQs
- Individuals who no longer need access should have their access disabled/removed in a timely fashion, especially depending on the sensitivity of the underlying data and the circumstances for the change in access requirements. This is particularly relevant for individuals who have transferred from one business unit to another or otherwise no longer have a job-related need for such access. This responsibility primarily lies with the dept/business unit/data
- For Redcap projects please contact the RedCap team to remove access for individuals who have separated, transferred to another business unit or are otherwise no longer authorized for such access. Please see UM REDCap or contact redcapadmin@med.miami.edu.
- Be sure to remove the data when feasible and no longer required (subject to any data retention requirements) at the end of the project.

Access

- All employees (usually but not exclusively UHealth) with access to PHI must complete HIPAA Privacy & Security Awareness training on an annual basis. This training is usually assigned via the University Learning Management system ULearn. For those who may not have ready access to ULearn, please visit UHealth Compliance- HIPAA Privacy & Security Awareness Training for External Learners. For issues/questions with the training or link, please contact the UHealth

Compliance Office at compliancеeducation@miami.edu**.** Jackson employees/residents should have completed mandatory HIPAA Privacy/Security training.

- Do not share your University of Miami credentials for accessing University of Miami systems with anyone.
- Only Remote access methods approved by UM IT should be used. This is particularly important if travelling, telecommuting, working from home, or otherwise using non-UM networks (wired and wireless). For more information, please refer to this UM IT article.
- For more information on Telecommuting and Remote Operations, please see Access UM's Network via UMIT's Approved Remote Access Tools as well as the Data Broker Telecommuting Guidelines.
- If mobile devices such as mobile phones or tablets are being used for access, these devices must utilize a PIN with a timeout/auto-lock. For more details, please see UM IT Mobile Device PIN.
- On University facilities/campuses, only use approved UM provided wireless networks. Please see UM Wireless networks.
- When conducting University/UHealth business, it is best to avoid solely using public, insecure wireless networks e.g. at coffee shops, airports, book stores, hotels etc. Connect to UM provided virtual private network (VPN) resources before conducting University business. The University’s VPN allows faculty, staff, and students to securely access and connect to the University's private network from anywhere through public networks, such as a non-University Internet Service Provider (ISP) or unsecured public wireless network. Connecting to a VPN while working remotely protects sensitive information and is required when accessing certain University applications. See UM VPN Information.

Data Transfer

- Do not use public email accounts (Gmail, Hotmail etc.) to send PHI, other sensitive data or conduct other University business.
- To encrypt e-mails from your UM Outlook account, type [secure] in the subject line. Make sure there is a space in between [secure] and other text in the subject line. See UM IT Office 365 Send/Retrieve Encrypted Email as well as UM IT Email Privacy FAQs.
- If there is a need for regular, authorized transfers of data, including especially to external recipients, but including inter and intra-campus, please contact the appropriate IT group, either UM IT (305-284-6565, help@miami.edu) or UHealth IT (305-243-5999, help@med.miami.edu). They will be able to recommend and implement appropriate solutions, including VPN tunnels or SFTP methods.

- Do not send PHI or other sensitive data to unauthorized individuals (i.e. individuals who have no business/clinical reason, no approved involvement in project etc.) or to individuals with non miami.edu or jhsmiami.org email addresses.
- Do not share any sensitive information with individuals outside University/UHealth unless an appropriate agreement (BAA, DUA, DTA, MTA, NDA, CDA, SRA, MOU etc.) approved by department/business unit leadership is in place. Such agreements should have review by an appropriate, applicable University/UHealth legal/regulatory/compliance area.
- For data transfers that potentially involve PHI/UHealth, please utilize this UHealth IT app HIPAA Request Tool to submit a request. Questions regarding this app can be sent to UHealth Cybersecurity or UHealth Help Desk.
- For on-line meetings e.g. via Teams or Zoom, be cautious with sharing links and/or data. Data should be shared or accessible only for individuals who are authorized for such access. Particular care should be exercised for meetings involving non-UM individuals. Remind attendees not to share sensitive information inadvertently, especially when sharing screens. Your video-conferencing software, just like other applications on your devices, should be consistently updated to reflect the latest version as supported and recommended by UM/UHealth IT. Please see:
    - https://www.it.miami.edu/a-z-listing/microsoft-teams/index.html
    - https://www.it.miami.edu/a-z-listing/zoom/index.html

Data Disclosure

For research requests, as per record keeping requirements, any disclosures made pursuant to an IRB waiver requires accounting for disclosure. You must prepare and submit to the UHealth Privacy Office a record of disclosure for each disclosure of patient information under a waiver of authorization by using the HIPAA Accounting for Disclosures form (HIPAA Attachment 45) located on the HSRO HIPAA page and UHealth Compliance/Privacy Office. For more than 50 individuals you can complete one accounting for disclosure form and a spreadsheet with patient names and MRN.