Storage

Sensitive Data	• 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.
Research Studies	• For research studies, please follow the data management section of the study protocol
De-Identified Data	• 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, telephone numbers, complete addresses and full facial photographs
Storage Access	• Securely store data sets and restrict 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.
Portable Devices	• 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 is now generally enabled for on-premises workstations. Consult the applicable IT group.
Anti-Malware	• An anti-malware application (e.g. CrowdStrike) should be installed and updated regularly on all University workstations. Confirm with IT, if necessary.
Mobile Devices	• 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. Pay attention to new advisories from IT as these practices are dynamic and being constantly updated.
Mobile Storage	• For mobile storage (USB Flash, hard drives) – avoid storing identifiable or confidential/sensitive data. • If you absolutely must, then such devices MUST be encrypted via a current, best practice encryption method/algorithm. 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 Storage and Documents	• 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. Again, please pay attention to announcements on updated practices from the appropriate area, be it Facilities or Records Management.

Home Location	• Avoid use of sensitive or identifiable paper documents at home, including printing of such documents. • Be aware of your surroundings when discussing Protected Health Information (PHI) to prevent inadvertent disclosure to unauthorized individuals nearby.
Unavoidable and Approved Use Case	• 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 or microcut shredder which is the preferred solution. • Again, AVOID use unless absolutely needed. NEVER dispose of University documents with identifiable or confidential/sensitive information in the regular trash.

Cloud Storage

University Approved 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/UM Single Sign-On (UMSSO) – NOT your personal Cloud accounts). • Contact IT for additional information, including learning resources for each solution.
Jackson Health	• 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.

Cloud Storage Sharing	• 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”.
	• It is best practice for individuals to have the minimum appropriate user access (i.e., view only, cannot share/print/download, etc.) to accomplish the purpose. Here are some useful links:
	  ○ OneDrive
	  ○ Box

Cloud Storage Access Removal	• 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 owner who controls the specific cloud folder/s.
REDCap Initiatives	• 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.

Data Removal	• Be sure to remove the data when feasible and no longer required (subject to any data retention requirements) at the end of the project. See the UM PI Manual available on the Human Subjects Research Office site and the University Records Retention schedule.

Access

HIPAA Privacy & Security Awareness Training	• All employees (usually but not exclusively UHealth) with access to PHI, and/or is located within a facility associated with the medical campus, 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 access to ULearn, and for additional questions, please contact the UHealth Compliance Office at complianceeducation@miami.edu. • Jackson employees/residents should have completed mandatory HIPAA Privacy/Security training.
Access Credentials	• Do not share your University of Miami credentials for accessing University of Miami systems with anyone.
Remote Access	• 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.
Telecommuting and Remote Operations	• 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.
Mobile Device PIN	• 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. • Pay attention to IT Advisories on updated guidance for mobile devices.
University Wireless Networks	• On University facilities/campuses, only use approved UM provided wireless networks. Please see UM Wireless networks.
Public Wireless Networks	• When conducting University/UHealth business, it is best to avoid using public, insecure wireless networks e.g. at coffee shops, airports, bookstores, 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

Public Email Accounts	• Do not use public email accounts (Gmail, personal Outlook, iCloud etc.) to send PHI, other sensitive data or conduct other University business.
Email Encryption	• 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.
Data Transfer Inter and Intra-campus	• 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.
Unauthorized Individuals	• 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.
Data Transfer Agreements	• 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 been reviewed by an appropriate, applicable University/UHealth legal/regulatory/compliance area.
Data Transfer External Entity	• For data transfers (received and/or transmit) to an external entity that potentially involve PHI/UHealth, please utilize the UHealth IT Cybersecurity HIPAA Request Forms (HIPAA Transmitting Form, HIPAA Receiving Form to submit a request. Questions regarding this app can be sent to UHealth Cybersecurity, UHealth Governance, Risk and Compliance or UHealth Help Desk.
Video Conferencing Applications	• 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

Research Request	• 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.

De-Identified Images

Data Privacy	• For Research studies, ensure that the privacy of participants is protected. • Important Note: While de-identification attempts to reduce the risk of identifying individuals, it may not completely eliminate it.
Agreements and Authorizations	• Submit proper agreements/Authorization/consents if identifiable images are being obtained. Such documents should clearly indicate under what conditions and with whom images can be shared.
De-Identification Process	• Document the de-identification process, including methods, storage, validation, and transfer of de-identified images to other parties if necessary
Identifiers Removal	• Follow the safe harbor guidance which includes removing all 18 types of identifiers listed by HIPAA, such as names, geographic subdivisions smaller than a state, all elements of dates (except year), and other unique identifying numbers or codes1. • Removal of Identifiers: Using image editing software, remove or obscure all direct and indirect identifiers such as faces, tattoos, scars, birthmarks, jewelry, clothing, photos of distinctive injuries, or other identifying features that could reveal the individual's identity. • Consult with UHealth IT for the latest de-identification image tools.
De-Identified Images Best Practices	• Guidance on deidentifying images in accordance with HIPAA, please refer to the OVPRS Research Privacy-Data Broker Best Practices: De-Identified Images document.

AI Tools

Accountability	• Assign clear responsibilities within the team for ethical AI use. • Grant access is based on user roles to protect sensitive data.
Informed Consent	• Obtain informed consent from participants to be fully informed regarding the use of the AI tool and/or model.
AI Documentation	• Document purpose/scope, model summary, data processing, key stakeholders, data sources, ethical, and privacy considerations.

Model Quality	• Perform AI model validation to meet the purpose/scope and verification of the model design and coding.
Data Privacy and Protection	• Only collect data that is necessary for the AI task. • Evaluate risks to privacy before deploying AI systems.
Bias and Ethics	• Regularly audit datasets for representation and fairness issues. • Use inclusive datasets that reflect the diversity of the population.
Research Studies	• For research studies, do not share or upload research data into any AI website that is not approved by the University.
AI Advisories	• This is a dynamic & rapidly evolving area so pay attention to the latest institutional advisories, tools and use cases.
UM AI Website	• Faculty, staff, and students to view the UMIT AI website, which offers comprehensive information about AI tools lists. • UMIT AI Main site: https://ai.it.miami.edu/index.html
AI Tools Review	• Faculty, staff, and students are encouraged to contact the UM AI Team for any inquiries or to request an AI tool review. Please reach out to the AI Team at ai@miami.edu.