The University of Texas MD Anderson Cancer Center
Information Resources and Data User Rights and Responsibilities Acknowledgement | December 2020

The University of Texas MD Anderson Cancer Center (MD Anderson) relies on its owned, leased, and controlled information resources (Information Resources) and the data contained within those systems (Data) to achieve its mission. This Information Resources and Data User Rights and Responsibilities Acknowledgement protects these Information Resources and Data in accordance with state law, The University of Texas System (UT System) Regents' Rules, and MD Anderson institutional policies and practices, and ensures that MD Anderson can access Data to fulfill its duties and mission. All individuals granted access to MD Anderson Information Resources and Data (Users) must be familiar with and follow the rights and responsibilities below.

Please note that many of MD Anderson's institutional policies are available online at www.mdanderson.org/hop.

A. General

MD Anderson Information Resources are provided for the express purpose of conducting the business and mission of MD Anderson.

Information stored on MD Anderson Information Resources may be shared only with others who have a business need to know such information, and such information may be shared only in compliance with applicable laws, regulations, and policies.

MD Anderson Information Resources must not be used to engage in acts against the mission and purposes of the institution; intimidate or harass; degrade performance; prevent access to institutional resources; obtain additional resources beyond those allocated; or circumvent security measures.

Information Resources must not be used to conduct a personal business or used for the exclusive benefit of individuals or organizations that are not part of UT System. Incidental personal use of certain systems is permitted; see Section F.

Inappropriate sexual or obscene materials must not be intentionally accessed, created, stored, or transmitted on MD Anderson Information Resources.

Users must not copy or reproduce any licensed software except as expressly permitted by the software license; use unauthorized copies on MD Anderson owned, leased, or controlled computers; or use software known to negatively impact MD Anderson Information Resources.

Use of smart phones or other devices to inappropriately capture Data in any format, including images, audio, and video, is prohibited.

Any exception to this agreement or Information Security policies must be approved by Information Security.

B. Data Protection and Data Integrity

All Data concerning any person, system, or asset of MD Anderson that is obtained or created in the performance of a User's duties is to the property of the Regents; may be confidential; and will not be disclosed to any individual unless such release of Data is directly related to the performance of the User's responsibilities.

Users may not further disclose Data without proper authorization or as required by law.

Data will be accessed and used only as necessary. Users of MD Anderson's Information Resources must not attempt to access Data or programs contained on Information Resources unless they have a business reason to do so.

To ensure the continued protection and integrity of Data, all Data will be documented and maintained in accordance with the Records Management Policy (MD Anderson Institutional Policy #ADM0107).

Confidential and Restricted Confidential Data, as defined by MD Anderson's Data Classification Guidelines & Ratings (*e.g.,* protected health information, research Data, student Data, Social Security numbers (SSNs)), must be stored and accessed only on MD Anderson Information Resources, in compliance with the Electronic Confidential and Restricted Confidential Information Access and Storage Policy (MD Anderson Institutional Policy #ADM1187). Confidential and Restricted Confidential Data that is transmitted through open networks (*e.g.*, the Internet and wireless networks) must be encrypted in accordance with MD Anderson's encryption guidelines. In conformity with federal guidance, MD Anderson research Data, as defined by MD Anderson Institutional Policy #ACA0014, must be stored and managed on MD Anderson Information Resources (including databases, systems, and applications conforming to the security policies above), and created and documented in English.

Databases that contain SSNs may not use SSNs as a primary key to the database. SSNs must not be displayed visually (such as on monitors, printed forms, and system outputs) unless required or permitted by law or by UT System-wide policy UTS165: Information Resources Use and Security Policy. Databases that contain SSNs may not use SSNs as the primary key to the database, or as a cross-reference to another key in the database. All use of SSNs must comply with the Protecting the Confidentiality of Social Security Numbers Policy (MD Anderson Institutional Policy #ADM0159).

MD Anderson's Electronic Health Record (EHR) consists of proprietary software that is owned exclusively by a commercial vendor and restricted from disclosure and dissemination to third parties. Accordingly, Users are prohibited from disclosing EHR object and source codes to unauthorized third parties. This includes ensuring that credentials used to access the EHR are kept confidential, and preventing the unauthorized copying or dissemination of EHR software, including screen displays.

Any User who needs to leave a computer or mobile device unattended must lock their User session and physically secure the computer or mobile device.

C. Information Services Privacy

Users have no expectation of privacy regarding any Data on or use of any MD Anderson owned, leased, or controlled Information Resources, including computers, servers, cloud storage, and email.

Data in any format residing on MD Anderson Information Resources or held on behalf of MD Anderson are owned by The University of Texas Board of Regents (Regents) and are subject to access by the institution and may be accessed without notice to comply with public information requests, court orders, subpoenas, or litigation holds; or for any other purpose consistent with the duties of the institution. Users have no expectations of privacy in any such Data, regardless of whether the Data were generated as the result of acceptable use (including incidental use as described in Section F) or unacceptable use of MD Anderson Information Resources.

Users are never compelled to use personally owned computers or mobile devices for institutional business.

MD Anderson acknowledges the privacy of Users with respect to personal information on personally owned computers and mobile devices to the extent possible, consistent with the business needs of the institution and obligations imposed by law. The expectation of privacy on personally owned computers and mobile devices differs in this respect from institutionally owned computers and mobile devices, on which MD Anderson Users have no expectation of privacy. Additionally, Users have no expectation of privacy regarding institutional Data residing on personally owned devices.

For additional information, see the Use of State-Owned Property, Equipment, Services, Funds, and Resources Policy (MD Anderson Institutional Policy #ADM0340).

D. Virus Protection

MD Anderson computers must have authorized and up-to-date virus protection software installed and enabled. Virus protection software will not be disabled or bypassed except as approved by Information Security. Computers or mobile devices found to be infected with a virus, ransomware, or other malicious software will be disconnected from the MD Anderson network until remediated and deemed safe by Information Security.

E. Email

The following email activities are prohibited:

- Using email for purposes of political lobbying or campaigning, except as permitted by Regents' Rules.
- Posing as someone other than oneself when sending email.
- Reading another User's email unless authorized to do so by the owner of the email account, or as authorized by policy for investigation, or as necessary to maintain services.
- Using email software that poses a security risk to other Users on MD Anderson's network.
- Sending or forwarding "chain" email.
- Sending email to more than 250 external (non-MD Anderson) recipients.
- Knowingly sending or forwarding email that is likely to contain computer viruses, malware, or ransomware.
- Sending Confidential or Restricted Confidential Data to external (non-MD Anderson) recipients without encryption.
- Sending credit card information via email.

F. Incidental Personal Use of Information Resources

Incidental personal use of email and Internet access is permitted by MD Anderson policy but is restricted solely to authorized Users; authorization does not extend to family members or acquaintances. Incidental personal use must not interfere with normal performance of a User's duties, must not result in direct costs to MD Anderson, and must not expose MD Anderson to unnecessary risks.

Users should not store personal files on MD Anderson Information Resources, including computers, servers, and cloud storage.

Users are reminded that all information, including personal information, that is shared through email or stored on Information Resources is discoverable under the Texas Public Information Act (TPIA) and Freedom of Information Act (FOIA).

G. Internet Use and Social Media

Internet browsers are provided to Users for business, education, research, and patient care purposes.

All User activity on the Internet will be subject to logging and review for network maintenance, performance monitoring, and ensuring compliance with applicable laws and policies.

Users sending emails, or posting to social media sites and other online content must not give the impression that they are representing, giving opinions, or making statements on behalf of MD Anderson unless authorized to do so. Users should use a disclaimer stating that the opinions expressed are their own and not necessarily those of MD Anderson. See MD Anderson's Social Media Policy (MD Anderson Institutional Policy #ADM1112) and Community Guidelines.

UT System-wide policy UTS122: Guidelines for Web Site Solicitations prohibits MD Anderson online content from displaying advertisements or statements implying that MD Anderson or UT System endorses goods, products, or services offered by a third party.

H. Remote Access

Users must adhere to all applicable Information Resources policies when remotely accessing Information Resources.

Personally owned computers may remotely access MD Anderson networks only through an institutionally approved Web portal. MD Anderson Information Resources may remotely access MD Anderson networks through a virtual private network (VPN) connection or through an institutionally approved portal.

All computers and mobile devices that access MD Anderson networks must be encrypted and secured in a manner consistent with MD Anderson policies.

If Information Security determines that a remotely connected computer or mobile device does not have required security-related software, has a virus, is party to a cyberattack, or in some way threatens the security of MD Anderson, the network connection will be disabled.

Users must not divulge MD Anderson remote access information and procedures to unauthorized individuals.

I. Cloud-based Systems and Services

Users may access MD Anderson cloud-based systems and services from non-MD Anderson-managed computers and mobile devices. However, Users must adhere to all Information Resources policies that apply to the management and control of institutional Data when doing so (*e.g.*, no storage of MD Anderson Data on non-MD Anderson-managed devices; no emailing of MD Anderson Data to personal email accounts, etc.). Information Security recommends that Users access MD Anderson cloud-based systems and services from MD Anderson-managed computers and mobile devices.

Information Security assesses and approves any implementation or use of cloud-based systems or services that utilize institutional Data. Users found to be using unapproved cloud-based systems or services to store, manage, manipulate, or share Data may have their accounts suspended and may be subject to corrective action.

When accessing any cloud-based system or service for MD Anderson purposes, Users must connect to such service using their MD Anderson accounts. If the cloud-based system or service supports local synchronization of Data, Users can synchronize Data only if using an MD Anderson-managed device. Users are prohibited from synchronizing personal information on MD Anderson-managed devices.

J. USB Mass Storage Devices

Data may never be stored or transported on USB mass storage devices (*i.e.*, USB devices that make it possible to store and transport large amounts of Data between computers) without prior authorization from Information Security. Additionally, USB mass storage devices may never be connected to an MD Anderson computer, network, or other Information Resources.

Users who have situations that require the use of USB mass storage devices must contact the Information Security department to complete an exception assessment.

K. Passwords

MD Anderson account, password, personal identification number (PIN), digital certificate information, security token, or any other similar information or device used for identification and authorization purposes must not be shared. Users are responsible for all activities conducted using their account.

L. Computer System Security

Except as authorized by the Information Security department, Users will not download or use security programs or utilities that reveal or exploit weaknesses in the security of a system, or that reveal Data by circumventing established authorization procedures. Password cracking programs, packet sniffers, and port scanners are prohibited on MD Anderson Information Resources. Users must report any suspected weaknesses in MD Anderson computer security and any incidents of possible misuse or violation of this agreement to an immediate supervisor, manager, department head, or the Information Security department.

Media containing Confidential or Restricted Confidential Data must be used, reallocated, and disposed of in a manner to prevent unauthorized access to the Data.

All Information Resources systems will be configured to display the MD Anderson authorized use notification at User login.

M. Incident Reporting

Users must report security incidents and suspected security incidents to 4INFO at 4info@mdanderson.org or 713-794-4636.

Users must report missing or stolen devices to UTP-H at 713-792-2890, and to 4INFO at 4info@mdanderson.org or 713-794-4636.

Users must report privacy concerns and suspected privacy concerns to the Institutional Compliance Office at 713-745-6636, or to the Compliance Hotline at 1-800-789-4448.

N. Preparatory to Research Attestation

Users who access MD Anderson Information Resources and use protected health information (PHI) for preparatory-to-research purposes (*e.g.,* development of research questions, determination of study feasibility, or identifying potential research participants) attest that no PHI will be removed from MD Anderson facilities or infrastructure, and that PHI is necessary for those preparatory-to-research purposes.

Please sign the appropriate attestation below.

Employees and Faculty Members: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as part of my personnel file; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in corrective action up to and including termination, and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Employee ID#: _____

Contingent Workers: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as part of my personnel file; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in termination of my contract with MD Anderson, and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Employee ID#: _____

Return this form to: _____

Representatives of Contract or Vendor Companies: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that anyone employed by my firm who accesses MD Anderson Information Resources must comply with this agreement, and I will inform all such employees of these requirements. I acknowledge that failure to comply may result in termination of my contract with MD Anderson, and/or action by law enforcement authorities.

Signature of authorized representative: _____ Date: _____

Printed name and title of authorized representative: _____ Vendor ID#: _____

Return this form to: _____

Adjunct or Visiting Faculty: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as a permanent record; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in termination of my position or status at MD Anderson, and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Employee ID#: _____

Students of the School of Health Professions: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as part of my student file; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in corrective action and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Student ID#: _____

Trainees (GME and Research): I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as part of my trainee file; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in corrective action up to and including termination, and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Trainee ID#: _____

Volunteers: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as part of my volunteer file; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in corrective action up to and including dismissal, and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Trainee ID#: _____

Research Study Monitors and other Regulatory Authorities: I acknowledge that I have received and read this MD Anderson Information Resources Acceptable Use Agreement. I understand that this document will be maintained as a permanent record; that I must comply with this agreement and other MD Anderson policies related to the use of any Data or information and all information systems; and that my failure to do so may result in termination of my access to MD Anderson Information Resources, and/or action by law enforcement authorities.

Signature: _____ Date: _____

Printed name: _____ Employer: _____