THE UNIVERSITY OF TEXAS
MD Anderson Cancer Center
Making Cancer History®

Data Classification Guidelines and Ratings

Published by Information Security and Institutional Compliance
Updated December 2020

MD Anderson classifies all its information (data) according to these Data Classification Guidelines and Ratings.

Data created by faculty, trainees, students, researchers, health care professionals and other MD Anderson employees are the property of the University of Texas Board of Regents – and therefore the State of Texas. The classification of any particular data reflects its value to the Regents and MD Anderson, and determines the extent to which we need to control and secure the data.

It's safest to think of all MD Anderson data as resources to be protected; no data should be shared with others unless there is a demonstrated, mission-specific need for such sharing. Err on the side of caution: Consider everything at least "Internal Use" until you confirm otherwise with the information owner. Anyone who does not adequately safeguard certain data may be subject to corrective action; see the Corrective Action Policy (#ADM0256).

Contact Information Security at security_risk@mdanderson.org with questions.

Public Data: Information obtained from the public domain or released to the public through authorized MD Anderson channels, such as Marketing or Communications. Public data are the least protected data type.

Impact to MD Anderson if compromised	Examples	Authentication Required	Minimum Retention Period[1]
Negligible adverse impact if the confidentiality, integrity, or availability of the data are compromised.	• **Online content:** Publicly accessible websites, links, and documents. • **Published or publicly presented data and research results:** Research papers that have been published in peer-reviewed publications; data that have been posted, uploaded, or submitted to public data registries.	User authentication is not required for access.	See the Texas State Records Retention Schedule.

Internal Use Data: Information intended to be generally used within MD Anderson, by MD Anderson workforce members – but that should not be released to the general public. Unauthorized use, such as copying-and-pasting institutional content (articles, sites, photographs) to external platforms may be a violation of copyright law.

Impact to MD Anderson if compromised	Examples	Authentication Required	Minimum Retention Period[1]
Minimal adverse impact if the confidentiality, integrity, or availability of the data are compromised.	• **Institutional policies and procedures not on MD Anderson's website,** mdanderson.org/hop. • **Employee phone directory** • **Internal sites and publications,** including Employee Notes	User authentication is recommended for access.	See the Texas State Records Retention Schedule.

Confidential Data: Information that is required by federal law, state law, UT System policies, Regents' Rules, MD Anderson policies, or MD Anderson contract terms to be maintained in a confidential manner. Confidential Data should be accessed only by a limited group of people. All data sets that contain protected health information (PHI) are considered Confidential Data, at a minimum. When Confidential Data is compromised (lost, stolen, disclosed without appropriate authorization), MD Anderson suffers a financial and reputational impact.

Impact to MD Anderson if compromised	Examples	Authentication Required	Minimum Retention Period[1]
Adverse impact if the confidentiality, integrity, or availability of the data are compromised.	• **MD Anderson financial information** • **MD Anderson facility information,** including as-built drawings, building security plans, utility diagrams, and security protocols • **PHI, ePHI[2], personally identifiable information (PII)** • **Research protocols and investigator brochures unless those are already publicly available on a public website such as Clinicaltrials.gov** • **Study records and study data for human subjects research studies including clinical research and clinical trials regardless of whether conducted under an Investigational New Drug (IND)[3] or Investigational Device Exemptions (IDE)[4] or not.** • **Invention disclosure reports** • **Unpublished manuscripts and articles** • **Non-public research protocols** • **Clinical practice protocols** • **Unfunded grant applications including those under NIH peer review** • **Sensitive or unpublished research data,** including information recorded in clinical trial case report forms, unpublished data, and unpublished research results • **Education (trainee and student) records**	User authentication is required for access.	See the Texas State Records Retention Schedule and the Medical Records Policy (#CLN0554).

Restricted Confidential Data: Building upon the Confidential Data classification, Restricted Confidential Data includes specific subsets of PHI and research data, as well as data related to credit cards and bank records. When Restricted Confidential Data is compromised (lost, stolen, disclosed), MD Anderson suffers a significant financial and reputational impact that may impair its mission.

Impact to MD Anderson if compromised	Examples	Authentication Required	Minimum Retention Period[1]
Significant adverse impact if the confidentiality, integrity, or availability of the data are compromised.	• **Mental health records** • **Drug abuse treatment records** • **AIDS or HIV test results** • **Genomic data,** including specific DNA markers that could identify an individual • **Payment Card Industry (PCI) information[5]** • **Passwords in any form or fashion** • **Information Security infrastructure, processes**	User authentication is required for access.	See the Texas State Records Retention Schedule and the Medical Records Policy (#CLN0554).

[1] Data owners are responsible for setting the retention schedule based on business needs, regulatory requirements, the Texas State Records Retention Schedule, and the Medical Records Policy (#CLN0554). The following records should be kept for at least six years:
   a. Policies and procedures (*e.g.*, our privacy and security policies, including certain standard operating procedures)
   b. Required communications (*e.g.*, authorizations, Joint Notice of Privacy Practices, acknowledgements)
   c. Actions, activities, or designations required to be documented (*e.g.*, privacy or security risk assessments, training, designations of a privacy officer)

[2] PHI that is transmitted or maintained electronically.

[3] Records for IND studies must be retained for a period of two years following the date a marketing application is approved for the drug for the indication for which it is being investigated; or, if no application is to be filed or if the application is not approved for such indication, until two years after the investigation is discontinued and the U.S. Food & Drug Administration (FDA) is notified.

[4] Records for IDE studies must be retained for a period of two years after the latter of the following two dates: The date on which the investigation is terminated or completed, or the date that the records are no longer required for purposes of supporting a premarket approved application or a notice of completion of a product development protocol.

[5] PCI data include complete credit card #, expiration date, card verification code, and personal identification number (PIN). The PIN must not be stored subsequent to authorization, even if encrypted.