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

DATA CLASSIFICATION GUIDELINES AND RATINGS

All M. D. Anderson information is classified according to this Data Classification Guidelines and Ratings. An owner of Information Resources has the responsibility to assess and classify the information. An owner is the designated person responsible for carrying out the program that uses the resources. Use these criteria to determine which data classification is appropriate for a particular information or infrastructure system The classification of the data should then determine the extent to which the data needs to be controlled/secured and is also indicative of its value to M. D. Anderson. For more detail information, please refer to the Information Security Department's Information Security Guidelines.

Data Classification	Definition	Criteria	Data Examples	Rating	Minimum Retention Period[1]
A **Public**	Information obtained from the public domain or released to the public through authorized channels. All data not classified in one of the three categories below, falls into the public designation by default.	Negligible adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	De-identified - (i.e., All 18 personal Identifiers [See **HIPAA Definitions Plan**] have been removed from the data, so that by looking at it, an individual person may not be identified or associated with it, and there is no reasonable basis to believe that the data can be used to identify an individual person) Aggregated - The data have been run through some Statistical/ Mathematical process. Published or Publicly Presented Subject Data and Results of Research - Research papers have already been Published in Medical Journals. Data have been posted to Public Data Registries). Information Technology - Publicly accessible websites, links, and documents, example: non-authenticated public pages.	A User Authentication is not Required.	See Records Retention Schedule
B **Internal Use**	Information intended to be generally releasable and used within M. D. Anderson, but should not be released to the general public.	Minimal adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	Clinical policies/procedures of M. D. Anderson or general policies/procedures of M. D. Anderson's Institutional Review Board ("IRB") - Protocol Review procedures, IRB policies and procedures. Employee phone list - Protocol staff roster details such as names, phone numbers, etc. Information Technology - Internal websites and links not requiring authentication. Internal documents, such as User Guides. Information may be restricted by group by "Need to Know". All Internal IP addresses with the exception of PCI IP	B User Authentication is recommended	See Records Retention Schedule

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

DATA CLASSIFICATION GUIDELINES AND RATINGS

Data Classification	Definition	Criteria	Data Examples	Rating	Minimum Retention Period[1]
			address range and others to be named. De-identified and non-confidential Research Data		
C Confidential	Information that, if compromised, would have a significant financial impact to M. D. Anderson, and violate federal or state law or the terms of confidentiality provisions in M. D. Anderson contracts. Information that should be accessed only by a limited group of people. All data sets that contain PHI receive this classification level, at a minimum.	Adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	Financial, PHI[2], ePHI[3], PII[4], Proprietary Information, Intellectual Property. Research Protocols and Investigator Brochures - Proprietary Protocol specific details such as Medications to be used, procedures to be used, etc, for ongoing protocols). Invention Disclosure Report. Sensitive Research Data - Information Recorded in Clinical Case Report Forms, etc. Unpublished Data and Results of Research). Student PII. Information Technology - -- "Administrator Need to Know Only": -- Application diagrams, Admin-level manuals, documentation, and diagrams for servers, workstations, databases, or applications; -- Administrator configuration procedures : server builds and hardening procedures; system configuration lists and reports; -- Network diagrams with confidential security information. -- Non-console administrative access by secure protocols and methods, which must use strong encryption. Website Consumer Information and information collected from the public including the following – -- First or last name; -- Address, including street name and city; -- Email address or other online contact information — like a screen name or IM user identifier; -- Phone number; -- Photos and videos; -- IP address, user ID, or other persistent identifier;	C User Authentication is Required.	See Records Retention Schedule and Retention of Medical Records Policy ADM0386 Study records for IND studies[5] Study records for IDE[6]

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

DATA CLASSIFICATION GUIDELINES AND RATINGS

Data Classification	Definition	Criteria	Data Examples	Rating	Minimum Retention Period[1]
			-- Physical location; -- Or any combination of those things		
D **Restricted Confidential**	Restricted Confidential builds upon the Confidential classification by addressing special access needs of a subset of PHI, such as mental health data. Restricted Confidential information should be accessed only by specific authorized people. Only the owner of the data may designate information sets as Restricted Confidential or grant access to this data.	Significant adverse impact to the institution, its patients, or employees resulting from confidentiality, integrity, or availability of the data being compromised.	Mental health, HIV - Specific diagnosis and treatment details which are covered by Doctor Patient confidentiality. Genomics - Specific DNA Markers etc that could identify an individual. Research Protocols Non-Public Unpublished Subject Data PCI[7] Information Technology – Passwords in any form, for any authentication method. Information Security information: -- Network diagrams showing locations of sensitive security and perimeter / border infrastructure devices; -- PCI IP address range and others to be named; -- Documentation showing or describing locations and configurations of information security or access infrastructure; -- Firewalls, Intrusion Detection and Protection systems locations, Border routers, internal switches and VLANs; -- Wireless access point, VPN, and remote authentication entry methods; -- Web access and SSL methods and configuration; -- Risk assessment and vulnerability reports, scan outputs; -- System and application logs.	D User Authentication is Required.	See Records Retention Schedule and Retention of Medical Records Policy ADM0386

[1] Data owners set the retention schedule based on business needs, regulatory requirements, Records Retention Schedule, as well as Retention of Medical Records Policy ADM0386
The following records should be kept for at least 6 years:
a. Policies and procedures (basically our privacy and security policies – include certain standard operating procedures)
b. Required communications (e.g., authorizations, NPP (Notice of Privacy Practices), acknowledgements, etc…)
c. Actions, activities, or designations required to be documented (e.g., risk assessments (privacy or security), training, designations of a privacy officer)

[2] Protected Health Information (PHI).

[3] Protected Health Information that is transmitted by or maintained in electronic media. (ePHI)
[4] Personally Identifiable Information (PII)
[5] Study records for investigational drug 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 FDA is notified.
[6] Study records for investigational device 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.
[7] Payment Card Industry (PCI) Complete credit card #, Expiration Date, Card Verification Code, and Personal Identification Number (PIN). The PIN and Personal Identification Number must not be stored subsequent to authorization (even if encrypted)