Data Classification Reference Guide

	Protected (highest, most sensitive)	Confidential (highly sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
Description	Protection of the information is required by law/regulation <u>or</u> the institution is required to self-report to the government and/or provide notice to the individual if information is inappropriately accessed	Data, information, or intellectual property in which Mount Sinai has a proprietary interest; or data protected by contractual obligations.	Data or information not generally available to the public.	Data for which there is no expectation for privacy or confidentiality.
*Data Examples (not all-inclusive) * exceptions apply*	**Protected Health Information (PHI)** • Health Status • Healthcare treatment, diagnosis • Healthcare payment • Medical Record Number • Date of Service • DOB • A face (video recording for research/educational purposes- i.e., reliability rating scales etc.) • Images collected as	**Information resources with access to confidential or restricted data (username and password).** Academic/Research Information • A grant application/ sections of a grant preparatory for submission for funding • Human subject information • Detailed annual budget information	**Personal/Employee Data** • Life number • Income information and Payroll information* • Personnel records, performance reviews, benefit information • Race, ethnicity, and/or nationality, gender • Date and place of birth • Directory/contact information designated by the owner as private	**Certain directory/contact information not designated by the owner as private.** • Name • [Addresses (campus and home)] I would think that home addresses would be Restricted, at least with the Medical Center as the source. • Email address • Listed telephone number(s) • Degrees, honors and awards • Most recent previous

	Protected (highest, most sensitive)	Confidential (highly sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
	part of diagnostic work ups (i.e., CT, MRI, Ultrasound) **Personally Identifiable Information (PII): Last name, and first name or initial, with any one of following:** • Social Security Number • Driver's license • State ID card • Passport number • Financial account (checking, savings, brokerage, CD, etc.), credit card, or debit card numbers **Personal/Employee Data** • Worker's compensation or disability claims **Student Data not included in directory information. This includes:** • Loan or scholarship	Management of data • Conflict of Interest Disclosures **Business/Financial Data** • Contracts – that don't contain PII • Information covered by non-disclosure agreements	**Business/Financial Data** • Financial transactions which do not include confidential data • Records on spending, borrowing, net worth • Policies and Procedures **Academic/Research Information** • Unpublished research or research detail/results that are confidential data; • Library transactions (e.g., circulation, acquisitions) • Private funding information • Course Evaluations **Management Data** • Medical Center's investment information	educational institution attended • Major field of study • Dates of current employment, position(s) • ID card photographs for University use **Specific for students:** • Class year • Participation in campus activities and sports • Weight and height (athletics) • Dates of attendance • Status **Business Data** • Campus maps • Job postings • List of publications (published research

	Protected **(highest, most sensitive)**	**Confidential** **(highly sensitive)**	**Restricted** **(moderate level of sensitivity)**	**Public** **(low level of sensitivity)**
	information • Payment history • Student tuition bills • Student financial services information • Class lists or enrollment information • Transcripts; grade reports • Notes on class work • Disciplinary action **Business/Financial Data** • Credit card numbers with/without expiration dates • Credit reports		**Systems/Log Data** • Server Event Logs	
Reputation Risk	Very High	High	Medium	Low
Data Access and Control	Data is accessible only to those individuals designated with approved access and otherwise consistent with	Data is accessible only to those individuals designated with approved access and otherwise consistent with	May be accessed by Mount Sinai employees and non-employees as part of their duties for Mount Sinai	No access restrictions. Data is available for public access.

	Protected (highest, most sensitive)	Confidential (highly sensitive)	Restricted (moderate level of sensitivity)	Public (low level of sensitivity)
	Mount Sinai policies	Mount Sinai policies		
Transmission	Transmission of Protected data on any non-Mount Sinai wireless or wired network (e.g., Internet), or Mount Sinai insecure Guest Network is prohibited. Use of the Medical Center's VPN is required. Transmission through a protected electronic messaging system (e-mail, instant messaging, text messaging) is required.	Transmission of Confidential data on any non-Mount Sinai wireless or wired network (e.g., Internet), or Mount Sinai insecure Guest Network is prohibited. Use of the Medical Center's VPN is required. Transmission through a protected electronic messaging system (e-mail, instant messaging, text messaging) is required.	Transmission of Restricted data through any non-Mount Sinai wireless or wired network, or Mount Sinai insecure Guest Network is strongly discouraged. Where necessary, use of the Medical Center's VPN is required. Transmission through a protected electronic messaging system (e-mail, instant messaging, text messaging) may be required.	No other protection is required for public information; however, care should always be taken to use all University information appropriately.
Storage	Storage of Protected data is prohibited on Non-qualified Machines and Computing Equipment unless approved by the Information Technology Security Department. If approved, IT Security approved encryption is required on mobile Computing Equipment. IT Security approved security measures are also required if the data is	Storage of Confidential data is prohibited on Non-qualified Machines and Computing Equipment unless approved by the Information Security Officer. If approved, IT Security approved encryption is required on mobile Computing Equipment. IT Security approved security measures are also required if the data is not stored on a IT	Level of required protection of Restricted data is either pursuant to Mount Sinai policy or at the discretion of the owner or custodian of the information. If appropriate level of protection is not known, check with Information Security Officer before storing Restricted data unencrypted.	No other protection is required for public information; however, care should always be taken to use all Medical Center information appropriately.

	Protected (highest, most sensitive)	**Confidential (highly sensitive)**	**Restricted (moderate level of sensitivity)**	**Public (low level of sensitivity)**
	not stored on a IT Managed Machine.	Managed Machine.		
Documented Backup and Recovery Procedures	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are required.	Documented backup and recovery procedures are not required, but strongly encouraged.	Documented Backup and Recovery Procedures are not required, but strongly encouraged.
Documented Data Retention Policy	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is required.	Documented data retention policy is not required, but strongly encouraged.
Audit Controls	Data Managers and Data Custodians with responsibility for Protected data must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access. They are also required to submit an annual report to the Information Security Officer outlining departmental security practices and training participation.	Data Managers and Data Custodians with responsibility for Confidential data must actively monitor and review their systems and procedures for potential misuse and/or unauthorized access. They are also required to submit an annual report to the Information Security Officer outlining departmental security practices and training participation.	Data Managers and Data Custodians with responsibility for Restricted data should periodically monitor and review their systems and procedures for potential misuse and/or unauthorized access.	No audit controls are required.

Institution Services Quick Reference Guide

If not specified below, contact the Information Security Office for guidance before using a service to store, process, or transmit Prohibited, Restricted, or Confidential data as defined above, noting that Data Governance Board (DGB) approval is needed in advance of handling Prohibited data on anything other than Qualified Machines. Some of the services below require additional components in order to qualify for the specified permitted data classifications. Click on the service link for details.

	Service	Protected	Confidential	Restricted	Public
Mount Sinai (Internally Hosted) Services	Default Home (H:) Drive (consider addressing C drive)	✓	✓	✓	✓
	Group Drive	✓	✓	✓	✓
	Minerva Minerva Archive System	✗ ✓	✗ ✓	✓ ✓	✓ ✓
	Bucket	✗	✗	[]	✓
	Data Warehouse	✓	✓	✓	✓
	Confluence/Wiki	✗	✗	✓	✓
	Email (with "Secure:" in subject line)	✓	✓	✓	✓
	Email and Calendar (without "Secure:" in subject line)	✗	✗	✓	✓
	SharePoint	✗	✗	✓	✓
	Voice Messaging	✗	✗	✓	✓
	VPN	✓	✓	✓	✓
	Full Disk Encrypted Systems	✓	✓	✓	✓
	Unencrypted Workstations	✗	✗	✓	✓
	xxx			✓	✓
	xxx	✓		✓	✓

	Service	Protected	Confidential	Restricted	Public
Third-Party (Externally Hosted) Services Vetted by Mount Sinai	Mount Sinai instance of Box.com	❌	✅	✅	✅
	Citrix Sharefile	✅	✅	✅	✅
	Mount Sinai instance of Box.com	❌	✅	✅	✅
	Mount Sinai instance of Office 365	❌	✅	✅	✅
	Mount Sinai instance of Azure	✅	✅	✅	✅
	Enterprise Google Apps (Calendar, Contacts, Docs, Drive, Email, Sites, and Talk)	❌	❌	✅	✅
	Google Apps (Calendar, Contacts, Docs, Drive, Email, Sites, and Talk)	❌	❌	❌	✅
	Dropbox (No Agreement)	❌	❌	❌	✅
	Amazon (No Agreement)	❌	❌	❌	✅
End User Devices	MDM Managed Devices	✅	✅	✅	✅
	Unmanaged Devices	❌	❌	❌	✅

✅Permitted ❌Not Permitted