Weill Cornell Medicine

11.03

Data Classification

Responsible Executive:	Chief Information Officer, WCM
Original Issued:	October 1, 2007
Last Updated:	November 19, 2021

Policy Statement

In order to protect the security and integrity of Weill Cornell Medicine (WCM) data, as well as to comply with applicable state and federal laws and regulations, all WCM data must be classified as either *high risk (confidential)*, *moderate risk (restricted),* or *low risk (public)*. Managers and administrators of information technology resources are responsible for this classification.

Reason for Policy

Information technology and data constitute valuable WCM assets. Depending on their classification, these assets are additionally subject to state and federal regulation. This policy is designed to provide a launching point for facilitating compliance with these regulations and adherence to commonly accepted security best practices.

Entities Affected by this Policy

Weill Cornell Medicine

Who Should Read this Policy

All individuals accessing, storing, sending, receiving, or transmitting any WCM data.

Web Address of this Policy

https://its.weill.cornell.edu/policies/

Contacts

Direct any questions about this policy, 11.03 – Data Classification, to Brian J. Tschinkel, Information Security Officer, using one of the methods below:

• Office:	(646) 962-2768
• Email:	brt2008@med.cornell.edu

Contents

1. Classifications

The following risk categorization levels must be adhered to when determining classification for data.

High Risk (Confidential)	Moderate Risk (Restricted)	Low Risk (Public)
• Protected health information • Personally identifiable information • Financial data • Employment records • Research data involving human subjects • Controlled Unclassified Information (CUI) • User account or system passwords providing access to above elements	• Student records, except where covered under high risk • Unpublished regulated research data • De-identified health-related research data • WCM operational data • WCM intellectual property • Donors or potential donors • Information security data • Other internal WCM data, limited by intention or discretion of author or owner	• WCM public websites • Public Directory data • Publicly available research data sets • Otherwise unrestricted research data • Press releases • Job postings

Please review the detailed bullets below for additional details.

1.01 High Risk (Confidential)

This includes data that could have a significant adverse impact on WCM's safety, finances, or reputation if improperly disclosed. Confidential data includes, without limitation, the following:

- Protected health information (PHI), as defined in Title 45 CFR §160.103, is individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information (i) in education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g; (ii) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.

- Personally identifiable information (PII), as defined in GAO-08-536 Privacy Protection Alternatives, is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

- Financial data, including data covered under the Gramm-Leach-Bliley Act (GLBA) and the information pertaining to credit cards covered by the Payment Card Industry Data Security Standard (PCI DSS).

- Employment records, including pay, benefits, personnel evaluations, and other staff records

- Research data involving human subjects that are subject to the Federal Policy for the Protection of Human Subjects (Common Rule) as defined in Title 45 CFR §46.101 et seq.

- Controlled Unclassified Information (CUI), as defined by the National Archives and Record Administration (NARA), is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

- User account or system passwords that provide access to information systems or applications containing any of the above confidential data elements.

1.02 Moderate Risk (Restricted)

This includes information that would not cause material harm, but has a moderate risk on WCM's safety, finance, or operations if improperly disclosed. Restricted data requires protection from unauthorized use, disclosure, modification, and/or destruction, but is not subject to any of the items listed in the confidential definition above. Data deemed restricted includes:

- Student records, including those protected under the Family Education Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, except where records are separately covered under confidential data.
- Unpublished data related to research and constrained by regulation or use agreements, unless containing elements in the high risk category or deemed high risk (confidential) by the oversight committees, including, but not limited to, the Institutional Review Board (IRB), Institutional Animal Care and Use Committee (IACUC), Institutional Biosafety Committee (IBC), Embryonic Stem Cell Research Oversight Committee (ESCRO), Radiation Safety Committee (RSC), or principal investigator.
- Health-related research data that has been de-identified in accordance with either the "Expert Determination" method [Title 45 CFR §164.514(b)(1)] or the "Safe Harbor" method [Title 45 CFR §164.514(b)(2)].
- Data related to Weill Cornell Medicine's operations, finances, legal matters, audits, or other activities of a sensitive nature not intended for public disclosure.
- Data related to intellectual property of Weill Cornell Medicine, which may be patented or used for financial gain.
- Data related to donors or potential donors.
- Information security data, including private cryptographic keys for data transfer or data at rest, system configuration documentation, infrastructure or network diagrams, vulnerability and penetration assessments, and other data associated with security-related incidents occurring at Weill Cornell Medicine, except where pertaining or providing access to systems containing data in the high risk category.
- Any other internal Weill Cornell Medicine data—the distribution of which is limited by intention or discretion of the author, owner, or administrator.

1.03 Low Risk (Public)

This includes data that can be disclosed to any individual or entity inside or outside of WCM, with minimal risk to WCM's safety, finance, or operations. Security measures may or may not be needed to control the dissemination of this type of data. Examples include:

- Data on public Weill Cornell Medicine websites, including data elements published as "Public" on the Directory (https://directory.weill.cornell.edu; see *ITS 11.13 – Directory* policy), such as email address, office phone number, office location, etc.
- Data related to research that is either published, publicly available, not intellectual property (as defined in moderate risk), or not constrained by regulation or use agreements.
- Press releases.
- Job postings.