COLUMBIA UNIVERSITY
DATA CLASSIFICATION POLICY

Published: October 2013
Revised: November 2014,
April 2016

I. Introduction

As indicated in the Columbia University Information Security Charter (the "Charter") http://policylibrary.columbia.edu/information-security-charter, any person who uses, stores or transmits Data (as defined in the Charter) has a responsibility to maintain and safeguard such Data.

The first step in establishing the safeguards that are required for a particular type of Data is to determine the level of sensitivity applicable to such Data. Data classification is a method of assigning such levels and thereby determining the extent to which the Data need to be controlled and secured.

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy History

The effective date of this Policy is November 1, 2013. This Policy replaces the University's Data Classification Policy, dated December 2007, as amended in February 2013.

III. Policy Text

Data security measures must be implemented commensurate with the sensitivity of the Data and the risk to the University if Data is compromised. It is the responsibility of the applicable Data Owner to evaluate and classify Data for which he/she is responsible according to the classification system adopted by the University and described below. If Data of more than one level of sensitivity exists in the same System or Endpoint, such Data shall be classified at the highest level of sensitivity.

A. Data Classification

The University has adopted the following four classifications of Data:

1. **Sensitive Data:** any information protected by federal, state or local laws and regulations or industry standards, such as HIPAA, HITECH, the New York State Information Security Breach and Notification Act, similar state laws and PCI-DSS.

For purposes of this Policy and the other Information Security Policies, Sensitive Data include, but are not limited to:

Personally Identifiable Information (PII): any information about an individual that (a) can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name or biometric records, (b) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual and (c) is protected by federal, state or local laws and regulation or industry standards.

Protected Health Information (PHI): any information created, received, maintained, processed or transmitted by the Columbia Health Care Component that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for health care and (a) identifies the individual or (b) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. The University's Office of the General Counsel and Office of HIPAA Compliance are responsible for determining whether particular information created, received, maintained, processed or transmitted by Columbia constitutes PHI.

Examples of Sensitive Data can be found in Appendix A hereto.

2. **Confidential Data:** any information that is contractually protected as confidential by law or by contract and any other information that is considered by the University appropriate for confidential treatment.

For purposes of this Policy and the other Information Security Policies, Confidential Data include, but are not limited to:

- Student education records that are directly related to prior, current and prospective University students and maintained by Columbia or an entity acting on Columbia's behalf, but not including (a) "directory information", such as a student's name, address, degrees and awards, subject to certain requirements as specified in FERPA and the University FERPA policies or (b) such records disclosed to school officials with legitimate educational interests or to organizations conducting certain studies on Columbia's behalf.

Human resources information, such as salary and employee benefits information

- Non-public personal and financial data about donors
- Information received under grants and contracts subject to confidentiality requirements
- Law enforcement or court records and confidential investigation records
- Citizen or immigrations status
- Unpublished research data
- Unpublished University financial information, strategic plans and real estate or facility development plans
- Information on facilities security systems
- Nonpublic intellectual property, including invention disclosures and patent applications
- Applicant financial information

3. **Internal Data:** any information that is proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data.

For purposes of this Policy and the other Information Security Policies, Internal Data include, but are not limited to:

- Internal operating procedures and operational manuals
- Internal memoranda, emails, reports and other documents
- Technical documents such as system configurations and floor plans

4. **Public Data:** any information that may or must be made available to the general public, with no legal restrictions on its access or use.

For purposes of this Policy and other Information Security Policies, Public Data include, but are not limited to:

- General access data on www.columbia.edu
- University financial statements and other reports filed with federal or state governments and generally available to the public
- Copyrighted materials that are publicly available
- Directory information under FERPA

B. Protection of Data

The protection requirements applicable to each classification of Data can be found in the Columbia University Registration and Protection of Systems Policy http://policylibrary.columbia.edu/registration-and-protection-systems-policy and/or the Columbia University Registration and Protection of Endpoints Policy. http://policylibrary.columbia.edu/registration-and-protection-endpoints-policy

IV. Cross References to Related Policies

The Information Security Policies referred to in this Policy are listed in Appendix B hereto.

Appendix A

Examples of Sensitive Data

Examples of PII include, but are not limited to, any information concerning a natural person that can be used to identify such natural person, such as name, number, personal mark or other identifier, in combination with any one or more of the following:

- Social security number
- Driver's license number or non-driver identification card number
- Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Email address with password (in certain narrow instances)

Examples of PHI include, but are not limited to, any health information, including demographic information about an individual, that includes any one or more of the following identifiers:

- Name
- Geographic subdivision smaller than a state
- Any element of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date or date of death
- Telephone number
- Fax number
- Electronic mail address
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate/License number
- Vehicle identifier and serial number, including license plate number
- Device identifier and serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Biometric identifier, including finger and voice print
- Full face photographic image and any comparable image
- Any other unique identifying number, characteristic, code or combination that allows identification of an individual.

Appendix B

Related Policies

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter

Registration and Protection of Endpoints Policy
http://policylibrary.columbia.edu/registration-and-protection-endpoints-policy

Registration and Protection of Systems Policy
http://policylibrary.columbia.edu/registration-and-protection-systems-policy