COLUMBIA UNIVERSITY
INFORMATION SECURITY CHARTER
Published: October 2013
Revised: November 2014

I. Introduction

In the course of carrying out its academic, research and clinical missions, faculty, staff and students at Columbia University (“Columbia” or the “University”) collect many different types of information, including financial, academic, medical, human resources and other personal information. The University values the ability to communicate and share information appropriately. Such information is an important resource of the University and any person who uses information collected by the University has a responsibility to maintain and protect this resource. Federal and state laws and regulations, as well as industry standards, also impose obligations on the University to protect the confidentiality, integrity and availability of information relating to faculty, staff, students, research subjects and patients. In addition, terms of certain contracts and University policy require appropriate safeguarding of information.

This Charter and the information security policies adopted by the University hereunder (collectively, the “Information Security Policies”) define the principles and terms of the University’s Information Security Management Program (the “Information Security Program”) and the responsibilities of the members of the University community in carrying out the Information Security Program. The current Information Security Policies are listed in Appendix A hereto.

The information resources (the “Information Resources”) included in the scope of the Information Security Policies are:

- All Data (as defined in Section IV below) regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);
- The computing hardware and software Systems (as defined in Section IV below) that process, transmit and store Data; and
- The Networks (as defined in Section IV below) that transport Data.

The Information Security Policies are University-wide policies that apply to all individuals who access, use or control Information Resources at the University, including faculty, staff and students, as well as contractors, consultants and other agents of the University and/or individuals authorized to access Information Resources by affiliated institutions and organizations.

Capitalized terms used herein without definition are defined in Section IV below.
II. Charter History

The effective date of this Charter is November 1, 2013. This Charter and the other Information Security Policies replace (A) the following University Policies:

- Information Security Charter, dated July 1, 2007
- Information Security Policy Statement

and (B) the following CUMC Policy:

- Information Security Charter, dated December 1, 2010

III. Charter Text

The mission of the Information Security Program is to protect the confidentiality, integrity and availability of Data. Confidentiality means that information is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of Data and processing methods. Availability means ensuring that authorized users have access to Data and associated Information Resources when required.

This Charter establishes the various functions within the Information Security Program and authorizes the persons described under each function to carry out the terms of the Information Security Policies.

The functions are:

A. Executive Management

Executive Managers are senior University officials, including the Provost, Deans, Executive Vice Presidents, Vice Presidents, Department Chairs, Institute or Center Directors and Senior Business Officers, who are responsible for overseeing information security for their respective areas of responsibility and ensuring compliance with all Information Security Policies. Such responsibilities include, but are not limited to:

- Ensuring that each System Owner and Data Owner in their respective areas of responsibility appropriately identify and classify Data in accordance with the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy;
- Ensuring that each such System Owner and Data Owner receives training on how to handle Sensitive Data and Confidential Data; and
- Ensuring that each IT Custodian in his/her area of responsibility provide periodic reports with respect to the inventory of Information Resources used in such area to the applicable Information Security Office.

B. Security, Policy and Compliance Governance
The following committees have been established to govern security, policy and compliance issues relating to the Information Security Program at the organizational level:

- Information Security Steering Committee (Executive Strategic Oversight)
- HIPAA Risk Committee (CUMC HIPAA/HITECH Risks and Compliance)
- University Compliance Committee (Regulatory Compliance Requirements)
- Administrative Policy Council (Review of and Advice on Administrative Policies)
- PCI-DSS Governance Committee (Credit Card Compliance)

C. Security Management

Security Managers are Managers in the Columbia University Information Security Office (the “CU Information Security Office”) and the Columbia University Medical Center Information Security Office (the “CUMC Information Security Office”; the CU Information Security Office and the CUMC Information Security Office being individually referred to as an “Information Security Office”). Security Managers are responsible for the day to day management of the Information Security Program, including:

- Developing, documenting and disseminating the Information Security Policies;
- Educating and training University personnel in information security matters;
- Communicating information regarding the Information Security Policies;
- Developing and executing the Risk Management Program;
- Collaborating with the University’s Office of HIPAA Compliance and HIPAA Privacy Officer on matters relating to PHI;
- Translating the Information Security Policies into technical requirements, standards and procedures;
- Collaborating with Data Owners and System Owners to determine the appropriate means of using Information Resources; and
- Authorizing any required exceptions to any Information Security Policy or any associated technical standards or procedures and reporting such exceptions to the Office of the General Counsel.

In addition to the responsibilities listed above, the Executive Managers have granted the authority to the Information Security Office to conduct the following activities:

- Monitoring communications and Data that use the University Network or Systems for transmission or storage;
- Monitoring use of the University’s Information Resources;
- Conducting vulnerability scanning of any Information Resources connected to the University Network;
- Conducting security assessments of Systems, Server centers and Data centers;
- Disconnecting Information Resources that present a security risk from the University Network;
- Erasing all Data stored on personal Endpoints previously used for University business, as requested or required; and

The University’s Information Security Officer and CUMC’s Information Security Officer are the Security Management responsible officers.

D. Data Ownership

Data Owners are University officials, including Directors, Officers of Instruction and Officers of Research, who are responsible for determining Data classifications, working with the applicable Information Security Office in performing risk assessments and developing the appropriate procedures to implement the Information Security Policies in their respective areas of responsibility. Such responsibilities include, but are not limited to:

• Appropriately identifying and classifying Data in their respective areas of responsibilities in accordance with the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy;
• Establishing and implementing security requirements for such Data in consultation with the applicable Information Security Office;
• Where possible, clearly labeling Sensitive Data and Confidential Data;
• Approving appropriate access to Data; and
• Ensuring that the Columbia University Sanitization and Disposal of Information Resources Policy http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy is followed.

E. System Ownership

System Owners are University officials, including Directors, Officers of Instruction and Officers of Research, who are responsible for determining computing needs, and applicable System hardware and software, in their respective areas of responsibility and ensuring the functionality of each such System. Such responsibilities include, but are not limited to:

• Classifying each System in their respective areas of responsibility based on the identification and classification of Data by the applicable Data Owner;
• Ensuring that each such System that contains Sensitive Data or Confidential Data is scheduled for risk assessment in accordance with the Columbia University Information Security Risk Management Policy http://policylibrary.columbia.edu/information-security-risk-management-policy;
• Establishing and implementing security requirements for each such System in consultation with the applicable Information Security Office;
• Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
• Maintaining an inventory of such Systems;
• Approving appropriate access to such Systems; and
• Ensuring that the Columbia University Sanitization and Disposal of Information Resources Policy http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy is followed.

F. Technical Ownership

IT Custodians are University personnel who are responsible for providing a secure infrastructure in support of Data, including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by Data Owners or System Owners and implementing and administering controls over Data in their respective areas of responsibility. Such responsibilities include, but are not limited to:

• Maintaining an inventory of all Endpoints used in their respective areas of responsibility;
• Conducting periodic security checks of Systems and Networks, including password checks, in their respective areas of responsibility;
• Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
• Performing self-audits and reporting metrics to the applicable Information Security Office and monitoring assessments and appropriate corrective actions; and
• Ensuring that the Columbia University Sanitization and Disposal of Information Resources Policy http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy is followed.

IT Groups are two or more IT Custodians whose responsibilities involve the same Information Resource. All IT Groups located within CUMC must follow the specific procedures relating to IT Groups in the CUMC Information Security Procedures.

G. System or Data Usage

Users are persons who use Information Resources. Users are responsible for ensuring that such Resources are used properly in compliance with the Columbia University Acceptable Usage of Information Resources Policy http://policylibrary.columbia.edu/acceptable-usage-information-resources-policy, information is not made available to unauthorized persons and appropriate security controls are in place.

IV. Definitions

As used in the Information Security Policies, the following terms are defined as follows:


Approved OHCA Email System: as defined in the Columbia University Email Usage Policy http://policylibrary.columbia.edu/email-usage-policy-1.

Columbia or the University: as defined in Section I of this Charter.
Columbia University Medical Center: the health care component of the University that is comprised of the colleges, schools and departments that perform covered health care provider functions and other departments to the extent that they perform services in support of those functions, as specified in the Health Care Component Designation adopted and approved by the Trustees of the University on June 7, 2003, as may be amended from time to time.

Confidential Data: any information that is contractually protected as confidential information and any other information that is considered by the University appropriate for confidential treatment. See the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy for examples of Confidential Data.

Covered Entity: as defined in the HIPAA Privacy Rule at 45 CFR 160.103.

CUMC/Hospital OHCA: The OHCA of which Columbia University Medical Center, NewYork-Presbyterian Hospital and Weill Cornell Medical Center are members.

CU Information Security Office: as defined in Section III(C) of this Charter.

CUIT: Columbia University Information Technology

CUMC: Columbia University Medical Center.

CUMC Information Security Office: as defined in Section III(C) of this Charter.


CUMC IT: Columbia University Medical Center Information Technology.

Data: all items of information that are created, used, stored or transmitted by the University community for the purpose of carrying out the institutional mission of teaching, research and clinical care and all data used in the execution of the University’s required business functions.

Data Owner: as defined in Section III(D) of this Charter.

Email System: a System that transmits, stores and receives emails.

Endpoint: any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the University wireless or wired Network, access Columbia email from any local or remote location or access any institutional (University, NewYork-Presbyterian Hospital, departmental or individual) System either owned by the University or by an individual and used for University purposes.

EPHI: Electronic Protected Health Information.

FERPA: the Family Educational Rights and Privacy Act
HIPAA: the Health Insurance Portability and Accountability Act and its implementing regulations as amended and supplemented by the HITECH Act and its implementing regulations, as each is amended from time to time.

HITECH: the Health Information Technology for Economic and Clinical Health Act

IDEA: the International Data Encryption Algorithm.

Information Resources: as defined in Section I of this Charter.

Information Security Office: as defined in Section III(C) of this Charter.

Information Security Policies: as defined in Section I of this Charter.

Information Security Program: as defined in Section I of this Charter.

Internal Data: as defined in the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy.

IP: Internet Protocol.

IT Custodian: as defined in Section III(F) of this Charter.

IT Group: as defined in Section III(F) of this Charter.


MAC: Media Access Control.

Mobile Device: a smart/cell phone (i.e., iPhone, Blackberry, Android, Windows phone), tablet (i.e., iPad, Nexus, Galaxy Tab and other Android based tablet) or USB/removable drive.

Network: electronic Information Resources that are implemented to permit the transport of Data between interconnected endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs and wireless access points.

OHCA: an Organized Health Care Arrangement, which is an arrangement or relationship, recognized in the HIPAA privacy rules that allows two or more Covered Entities that hold themselves out to the public as participating in a joint arrangement and participate in certain joint activities to share PHI for joint health care operations purposes.
**Payment Card:** for purposes of PCI-DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa, Inc.

**PCI:** Payment card industry.

**PCI-DSS:** the PCI Data Security Standard produced by the PCI–SSC, which mandates compliance requirements for enhancing the security of payment card data.

**PCI-SSC:** the PCI Security Standards Council, which is an open global forum of payment brands, such as American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc, that are responsible for developing the PCI-DSS.

**Peer:** a network participant that makes a portion of its resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by Servers or stable hosts. Examples include KaZaa, BitTorrent, Limewire and Bearshare.

**Peer-to-Peer File Sharing Program:** a program that allows any computer operating the program to share and make available files stored on the computer to any machine with similar software and protocol.

**PHI:** as defined in the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy.

**PII:** as defined in the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy.

**Public Data:** as defined in the Columbia University Data Classification Policy http://policylibrary.columbia.edu/data-classification-policy.

**Removable Media:** CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices and copiers.

**Risk Analysis:** The process of identifying, estimating and prioritizing risks to organizational operations, assets and individuals. “Risk Assessment” is synonymous with “Risk Analysis”.

**Risk Management Program:** The combined processes of Risk Analysis, Risk Remediation and Risk Monitoring.

**Risk Monitoring:** The process of maintaining ongoing awareness of an organization’s information security risks via the risk management program.

**Risk Remediation:** The process of prioritizing, evaluating and implementing the appropriate risk-reducing security controls and countermeasures recommended from the risk management
process. “Risk Mitigation” or “Corrective Action Planning” is synonymous with “Risk Remediation”.

**RSA**: the Rivest-Shamir-Adleman Internet encryption and authentication system.

**Sensitive Data**: any information protected by federal, state and local laws and regulations and industry standards, such as HIPAA, HITECH, FERPA, the New York State Information Security Breach and Notification Act, similar state laws and PCI-DSS. See the Columbia University Data Classification Policy [http://policylibrary.columbia.edu/data-classification-policy](http://policylibrary.columbia.edu/data-classification-policy) for examples of Sensitive Data.

**Server**: any computing device that provides computing services, such as Systems and Applications, to Endpoints over a Network.

**SMTP**: Simple Mail Transfer Protocol, which is an internet transportation protocol designed to ensure the reliable and efficient transfer of emails and is used by Email Systems to deliver messages between email providers.

**SSL**: the Secure Sockets Layer security protocol that encapsulates other network protocols in an encrypted tunnel.

**Student Education Records**: as defined in the Columbia University Data Classification Policy [http://policylibrary.columbia.edu/data-classification-policy](http://policylibrary.columbia.edu/data-classification-policy).

**System**: Server based software that resides on a single Server or multiple Servers and is used for University purposes. “Application” or “Information System” is synonymous with “System”.

**System Owner**: as defined in Section III(E) of this Charter.

**UPS**: Uninterruptible Power Supply.

**User**: as defined in Section III(G) of this Charter.

**User ID**: a User Identifier.

**VPN**: Virtual Private Network.

**V. Enforcement**

Violations of the Information Security Policies may result in corrective actions which may include: (a) the immediate suspension of computer accounts and network access; (b) mandatory attendance at additional training; (c) a letter to the individual’s personnel or student file; (d) administrative leave without pay; (e) termination of employment or non-renewal of faculty appointment or student status; or (f) civil or criminal prosecution.
VI. Applicable Laws, Regulations and Industry Standards

The federal and New York State laws and regulations and industry standards that are applicable to information security at the University are listed in Appendix B hereto.
Information Security Charter
http://policylibrary.columbia.edu/information-security-charter

Acceptable Usage of Information Resources Policy
http://policylibrary.columbia.edu/acceptable-usage-information-resources-policy

Business Continuity and Disaster Recovery Policy

Data Classification Policy
http://policylibrary.columbia.edu/data-classification-policy

Electronic Data Security Breach Reporting and Response Policy

Email Usage Policy
http://policylibrary.columbia.edu/email-usage-policy-1

Information Resource Access Control and Log Management Policy
http://policylibrary.columbia.edu/information-resource-access-control-and-log-management-policy

Information Security Risk Management Policy

Network Protection Policy
http://policylibrary.columbia.edu/network-protection-policy

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

Sanitization and Disposal of Information Resources Policy
http://policylibrary.columbia.edu/sanitization-and-disposal-information-resources-policy

Social Security Number (SSN) Usage Policy
http://policylibrary.columbia.edu/social-security-number-ssn-usage-policy
Federal

The Digital Millennium Copyright Act

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

The Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999)
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

The Health Insurance Portability and Accountability Act (HIPAA)
The Health Information Technology for Economic and Clinical Health Act (HITECH)

New York State

New York State Information Security Breach and Notification Act
http://www.dhsses.ny.gov/ocs/breach-notification/

Social Security Number Protection Law, 309-DDD and 309-DDD*2
http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$GBS399-DDD$$@TXGBS0399-DDD+&LIST=SEA14+&BROWSER=EXPLORER+&TOKEN=08146486+&TARGET=VIEW

Industry Standards

Payment Card Industry/Data Security Standard
https://www.pcisecuritystandards.org/tech/