Enterprise Information Technology Services
Information Security & Risk Management:
Information Technology Resources
Acceptable Use Policy

Effective Date: March 15, 2016

Review Frequency: Annually

Revised: January 31, 2022

Document Reference:
NYC Health + Hospitals_Enterprise IT_ISRM_Policy_002.5

1. Goal

Acceptable organizational and secure use of NYC Health + Hospitals (the System) information technology (IT) resources is required of all Workforce Members in order to minimize the System's exposure to information security risks. The objective of this Policy is to identify the System's IT resources acceptable use standards

2. Scope & Applicability

- The scope of this Policy includes all NYC Health + Hospitals IT resources.
- This Policy applies to all Workforce Members. Without exception, all Workforce Members are required to read, abide by, and acknowledge this Policy (see page 11).

3. Policy Authority

The NYC Health + Hospitals Chief Information Officer (CIO) has the authority to oversee, direct and coordinate the establishment and implementation of Enterprise Information Technology Services (Enterprise IT) Policies, Standards, and Guidelines for the System.

4. Definitions

Business Associate: A Business Associate is a person or entity, other than a Workforce Member, that performs functions or activities on behalf of, or provides certain services to the System that involve access by the Business Associate to Protected Health Information (PHI). A Business Associate may also be a subcontractor that creates, receives, maintains, or transmits PHI on behalf of a Business Associate. Examples of Business Associates include a Health Information Exchange or an information technology service provider who has access to NYC Health + Hospitals electronic systems, or a software provider that acts as an e-prescription gateway to a pharmacy.

Data Classification: Refers to the categorization of data based on its level of sensitivity and the impact to the System should that data be disclosed, transferred, altered and/or destroyed with or without proper approval and/or authorization. The baseline security controls that are implemented to safeguard data are determined by its classification. Data is generally classified into three (3) security categories:

1. ***Restricted Data* (*High Sensitivity*)**: Refers to data that has been classified as *confidential,* due to its high level of sensitivity, by law, policy or contractual obligation. Unauthorized disclosure, alteration or destruction of *restricted data* could result in a *high level of risk*. Examples of *restricted data* include, but are not limited to:
    - Personally, Identifiable Information (PII): Social Security Numbers (SSN), date of birth, payment card cardholder data, financial information, etc.
    - Protected health information (PHI)
    - Workforce Member employment records

   The highest level of security controls should be applied to this type of data.
2. ***Private Data* (*Moderate Sensitivity*)**: When the confidentiality of data is preferred due to its *moderate sensitivity level* it is classified as *private*. Unauthorized disclosure, alteration or destruction of private data could result in a *moderate level of risk*. Examples of *private data* include, but are not limited to:
    - Proprietary Data: Business and marketing plans, contracts, business processes, meeting minutes, budgets, etc.
    - Physical Site Plans
    - Hospital Police Security Plan
    - Information Security Program Plan

   By default, all data that is not explicitly classified as *restricted* or *public data* should be treated as *private data*. A reasonable level of security controls should be applied to this type of data.

3. ***Public Data* (*Non-Sensitive*)**: Data should be classified as *public* when the unauthorized disclosure, alteration or destruction of that data would result in *limited or no risk* to the System. Examples of public data include, but are not limited to:
   - Press Releases
   - Research Publications
   - List of Services Provided

   While little or no controls are required to protect the confidentiality of *public data*, some level of control is required to prevent unauthorized modification or destruction of *public data*.

IT Resource (Asset): Pertains to devices, computing equipment, infrastructure, information systems and applications that comprise the NYC Health + Hospitals network and all the electronic information (data) and communication contained within the network. IT resources include, but are not limited to, personal computers (PCs), mobile IT devices (laptops, smart phones, etc.), storage devices (external hard drives, USBs, etc.) scanners, printers, digital copiers, servers, information systems, applications, local and wide area network (wired or wireless).

Management: Within the context of this Policy, *Management* refers to Workforce Members whose responsibilities include leading and directing the System's resources (human, financial, and/or material).

Personal Device: For the purpose of this Policy, a personal device refers to a device, specifically, PC, laptop, smart phone, tablet, or portable storage device (i.e., external hard drive and USB thumb drive) that is owned by the Workforce Member, and not by NYC Health + Hospitals.

Personal Use: Covers any activity that is conducted for purposes other than accomplishing official work-related responsibilities/activities.

Port Forwarding: Refers to the technique of redirecting a communication request from one network port (communication endpoint within a network) to another. While there are valid reasons for using this technique, port forwarding can result in a security vulnerability that may easily allow a bad actor (hacker) to gain unauthorized access to a network.

Protected Health Information (PHI): Refers to any information, including demographic information and genetic information, whether oral or recorded in any form or medium, created or received by the System, or by business associates on behalf of the System 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 the provision of health care to an individual, and that also identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify an individual. PHI does *not* include health information in employment records held by the System in its role as employer or information concerning an individual who has been deceased for more than 50 years.

Remote Access: Refers to the ability to access IT resources from a remote (off-site) location via the use of the System's enterprise remote access solution.

Router: A router is an intelligent device that defines the desired communication path for data traffic within a network, or between, or across multiple networks. In addition, routers typically function as a firewall (barrier between a trusted and untrusted network) and are a central connecting point to the Internet.

System Business Contact: In relation to this Policy a *System Business Contact* refers to an individual or entity that the System engages with for business purposes. A *System Business Contact* may include, but may not be limited to, business partners, vendors, external counsel, advocacy groups, and regulatory bodies.

User: Refers to an individual who has been granted authorized access to one or more NYC Health + Hospitals IT resource(s).

Vendor: An individual or entity that provides a product and/or service to the System. Generally speaking, the term relates to an individual or entity that has been hired to deliver and has been paid for a product and/or a service provided.

Workforce Member (Personnel, or Workforce): Refers to individuals (whether serving in a temporary or permanent capacity on the System's premises or remotely) who perform duties, functions or activities (whether on a full-time, part-time, or per diem basis) on behalf of the System and whose conduct (in the performance of work functions and duties on behalf of the System) is under the direct control of the System (whether or not paid directly by the System). Examples include, but are not limited to: employees, volunteers, trainees, interns, and members of NYC Health + Hospitals Board of Directors.

5. Policy Statement

The following represents the IT resource acceptable use controls that have been adopted by the System, and must be complied with by all Workforce Members regardless of device type used (*System owned* vs. *personal device*), and Workforce Member work location (*System owned/managed facility* vs *Workforce Member owned/managed location*).

A. Access Control

1. Workforce Members shall not access, store, disclose, transmit, alter or destroy the System's IT resources without authorization.
2. Unauthorized access to the System's IT resources may constitute a civil or a criminal offense, and is a violation of the System's Policies, specifically:
   a. HIPAA Security Operating Procedures:
      - *250-17: HIPAA Security Policy - Integrity*
      - *250-19: HIPAA Security Policy - Transmission Security*

   b. *Enterprise Information Technology Services (Enterprise IT), Information Security & Risk Management (ISRM): Access Control Policy*
3. The System's IT resources may never be used to perform any action or activity that: violates federal, state or local laws (including copyright laws and licensing agreements), is in violation of the System's Policies, or poses an information security risk to the System.
4. Enterprise IT shall create, amend, or disable Workforce Member access to IT resources only when requested and authorized by Human Resources (HR) or Management.
5. Workforce Members who telecommute are required to ensure that the network they regularly use to access the System's IT resources is secured with a router that is:
   a. Protected with strong authentication and authorization methods as recommended by the Workforce Member's Internet Service Provider (ISP).

   b. Configured in a manner that helps prevent unauthorized access to the Workforce Member's device (desktop, laptop, etc.) from the outside (the Internet).
      - ➢ One way to accomplish this is to ensure *port forwarding* is disabled when configuring a router. If left enabled port forwarding may create a path of attack for a bad actor (hacker).
      - ➢ Telecommuting Workforce Members are responsible for working with their ISP and/or their router manufacturer to ensure secure network and router configuration.
6. In the event of a security related concern or suspected policy violation the System reserves the right to suspend a Workforce Member's access to IT resources without notice.

B. Password and Access Codes

1. Workforce Members shall only use their own uniquely assigned login credentials and shall never share their login credentials and/or other assigned authentication mechanisms (e.g., access ID cards, tokens, biometrics, etc.) with anyone.
2. When login technology requires the use of a password or an access code, Users shall create passwords or access codes that comply with the System's Enterprise IT-ISRM*: Password and Access Code Standard.*
3. Workforce Members must safeguard the confidentiality of their password(s) or access code(s) at all times; shall immediately report to Management any compromise or suspected compromise of their password(s) or access code(s), and shall immediately change their password or access code when a compromise is suspected or confirmed.

C. User Privacy Expectations

1. Workforce Members shall not have any privacy rights regarding the data they create, receive, maintain, or transmit while using the System's IT resources.
2. The System may record or review user access and usage of its IT resources as required without notice to or user consent.
3. The System reserves the right to comply with legal requests that may include, but may not be limited to, disclosing user electronic mail content, Internet access or browsing activity, and electronic files without user knowledge or consent.

D. Limited Personal Use

1. Limited personal use of the System's IT resources *is permitted only* when:
   a. use is not prohibited pursuant to this or another applicable System Policy,
   b. it does not interfere with or otherwise impede the health System's operations or Workforce Member productivity,
   c. it involves no more than a minimal expense (e.g., making a photocopy, printing a few pages, making a personal phone call, etc.) to the System; and
   d. it does not attribute the user's personal activity for instance, on social media or email, to NYC Health + Hospitals.
2. Limited personal use is *strictly prohibited* when said personal use:
   a. is prohibited by applicable law, rule, regulation, or NYC Heath + Hospitals' Policies or Operating Procedures.
   b. disrupts the normal operation of IT resources. Disruption includes, but is not limited to, network sniffing, ping floods, packet spooking, denial of service and forge routing information for malicious purposes.
   c. interferes with, or causes a disruption to the System's IT resources,
   d. is for the purpose of gaining unauthorized access to other IT resources,
   e. results in personal gain or is for personal business purposes, and
   f. is deemed as inappropriate, or offensive behavior/activity in the workplace.
3. Limited personal use of IT resources is a privilege and may be limited or revoked at any time.
4. Questions pertaining to limited personal use are to be submitted to Management.
5. Limited personal use of the System's IT resources is at the sole risk of the Workforce Member. The System is not responsible for any loss or damage resulting from such personal use.

E. Information Technology Resources

1. The following requirements and information security controls apply to Workforce Member use of System *owned* and/or *issued* IT resources:
   a. Data that is created, received, maintained, or transmitted on the System's IT resources is the property of the System.

b. Workforce Members are required to protect the System's IT resources against unauthorized access, loss, theft, and destruction at all times.
c. Lost or compromised IT resource constitutes a security incident and must be addressed as noted under *Section 6.2* of this Policy.
d. IT resources shall be configured with security configurations that comply with the System's standard.
e. Altering the security configuration settings of IT devices is strictly prohibited.
f. Removal of IT resources from NYC Health + Hospitals facilities requires Management approval (this excludes mobile devices issued to the user, e.g., laptop, smartphone, portable storage device, etc.).
g. Disposal or reallocation of IT devices by anyone other than Enterprise IT Team Members is strictly prohibited.
h. Upon termination of employment or affiliation with NYC Health + Hospitals, all System issued IT devices must be returned to Management or Human Resources.

2. User requirements and information security controls applicable to the use of *authorized personal devices* are defined in the *Enterprise IT-ISRM: Bring Your Own Device (BYOD) Policy.*

F. Email & Other Communication Apps

1. Workforce Members must use their NYC Health + Hospitals issued email account (@nychhc.org) to conduct business on behalf of the System.
2. Workforce Members may never use their personal email account (Yahoo, Gmail, Hotmail, etc.) to conduct business on behalf of the System.
3. Workforce Members may not use their NYC Health + Hospitals issued email account (@nychhc.org) to conduct personal business.
4. Workforce Members who are employees of a System Affiliate (i.e., NYU Langone, PAGNY, etc.) must use their System issued email account to conduct business on behalf of the System.
5. Workforce Members who are employees of a System Business Associate, or Vendor may only use their Business Associate or Vendor issued email account to conduct business on behalf of the System when permitted (and as specified) by their Business Associate Agreement, or goods or service contract with the System.
6. Workforce Members may use their System issued email account to internally (from their @nychhc.org email account to another @nychhc.org email account) transmit PHI when it is absolutely necessary in order to conduct business on behalf of the System. The following guidelines must be adhered to:
   - PHI transmitted is the minimum necessary required to complete role-based, Management authorized task(s).
   - Recipient name and electronic address of intended recipient has been verified prior to transmitting PHI.
7. The System's *restricted* or *private* data may only be transmitted to an external email account by creating a document (Word, Excel, PowerPoint, etc.) that is uploaded to and transmitted by the System's secure file transfer solution (kiteworks).
   - Workforce Members may not include the System's *restricted* or *private* data in any section (subject line, body, or file name of an attached document) of an email (even when encrypted) that is being transmitted to an external email account.
   - This restriction applies to the notification message that is generated and transmitted to an external email account by the System's secure file transfer solution (kiteworks).

8. When a legitimate business purpose exists for transmitting restricted or private data to a System Business Contact's personal email account an ISRM Policy Exception Request (see Section 7) must be processed, and an Enterprise IT approved secure file transmission method must be used.
9. The following may not be used to create, receive, maintain or transmit PHI:
    - document sharing or storage applications (i.e., Dropbox, Google Drive, iCloud, etc.) that are not authorized for use by Enterprise IT
    - phone texting apps that are not authorized for use by Enterprise IT
    - chatting apps (i.e., WhatsApp, Snapchat, etc.) that are not authorized for use by Enterprise IT.
10. Workforce Members may not use their NYC Health + Hospitals issued email account (@nychhc.org) to create *personal use* login accounts (i.e., personal banking account, personal mobile phone carrier account, personal online shopping account, personal social media account, etc.).
11. Use of NYC Health + Hospitals email system to send chain letters, email spam, inappropriate messages, or unapproved newsletters and broadcast messages is prohibited.
12. Users shall exercise extreme caution when clicking on links and/or opening attachments within an email in order to protect the System's IT resources.

H. Internet

1. Use of the System's Internet access must be consistent with the goals of NYC Health + Hospitals' business activities, or to facilitate information access or transfer of information as related to the job function of a Workforce Member.
2. NYC Health + Hospitals reserves the right to disallow access to any site (including Internet storage sites) that may harm or be inconsistent with the System's Policies, practices, and goals.
3. Transmitting or uploading the System's *restricted* or *private* data to an unauthorized *cloud-based storage system* (e.g., Dropbox, Google Drive, etc.) is prohibited.
4. Use of cloud computing services shall comply with the System's:
    - *Enterprise IT-ISRM: Security Policy on Cloud Computing Services*
    - *Enterprise IT-ISRM: Cloud Computing Security Standard*

I. Software

1. Only software that is authorized and managed by Enterprise IT may be installed on the System's IT resources.
2. Downloading unauthorized software onto IT resources is prohibited.
3. Unauthorized duplication of the System's software is strictly prohibited and is subject to civil and criminal penalties.

J. Public Forums (Blog Postings, Bulletin Boards, Twitter, Facebook, etc.)

1. Unauthorized disclosure of the System's *restricted* or *private* data is strictly prohibited.
2. The System's email addresses issued to Workforce Members for the purpose of conducting the System's business shall not be used for personal activities on public forums.
3. Workforce Members must comply with the System's *Operating Procedure 20-61: Social Media Use Operating Procedure* at all times.

6. Workforce Member Responsibilities

All Workforce Members are required to:

1. Contact the Enterprise Service Desk (ESD) at EnterpriseServiceDesk@nychhc.org, or by phone at 877-934-8442 immediately to report confirmed or suspected security incidents, which include but are not limited to: theft, vandalism, or loss of IT resources; policy violations; or compromised access accounts (an account that is being used by someone other than the Workforce Member it was issued to). Incidents that may require a greater degree of confidentiality may be reported directly to the ISRM Department via email at CISO@nychhc.org.
2. Report incidents related to unauthorized acquisition, access, use or disclosure of PHI per the procedures outlined in *NYC Health + Hospitals HIPAA Privacy Operating Procedure 240-08: HIPAA Policy: Privacy-Related Complaints*. Questions related to this Policy or referenced Operating Procedures may be directed to your supervisor, your facility's Compliance Officer, or to the Corporate Privacy and Security Officer (CPSO) at CPO@nychhc.org.
3. Report incidents related to criminal activity, corruption, conflicts of interest and violations of NYC Health + Hospitals rules, regulations or internal procedures to the Office of the Inspector General as outlined in *NYC Health + Hospitals Operating Procedure 30-1: Office of the Inspector General*.
4. Read and abide by the referenced NYC Health + Hospitals Operating Procedures and ISRM: Information Security Policies and ISRM: Information Security Standards, upon gaining access to the NYC Health + Hospitals Intranet and completing required HIPAA Privacy & Security Training.
5. Comply with all NYC Health + Hospitals Policies and Operating Procedures.

7. Exceptions

In the event adherence to this Policy (in part or in its entirety) is not feasible, an *Enterprise IT-ISRM Exception Request* shall be submitted to ESD. The request must include a detailed business justification, and when applicable and feasible, a description of the security safeguard(s) that will be implemented to mitigate any potential security risk(s) associated with the request. *Exception Requests* will be reviewed by the Corporate Chief Information Security Officer (CISO) (or his/her designee) and the CPSO. The CISO (or his/her designee) shall maintain a record of approved *Exception Requests*.

8. Compliance

Penalties for violating this Policy may result in:

- Termination of IT resources access privileges.
- Disciplinary action up to and including termination of employment, contract, or other affiliation with NYC Health + Hospitals.
- Criminal or civil penalties.

9. Related NYC Health + Hospitals Operating Procedures, Information Security Policies and Information Security Standards:

Operating Procedures:

http://hhcinsider.nychhc.org/corpoffices/syswidePnP/Pages/Index.aspx

- 20-58: Information Systems Application Access Policy & Procedure
- 20-60: Limited Personal Use of HCC Office and Technology Resources
- 20-61: Social Media Use
- 20-62: Telecommuting

- 50-01: Corporate Compliance and Ethics Program
- 250-01: HIPAA Security Policy-Security Risk Analysis, Management and Evaluation
- 250-05: HIPAA Security Policy-Workstation and Workforce Procedures
- 250-16: HIPAA Security Policy-Access and Authentication Procedures
- 250-17: HIPAA Security Policy-Integrity
- 250-19: HIPAA Security Policy-Transmission Security
- 250-20: HIPAA Security Policy-Remote Use and Access to Electronic Protected Health Information

ISRM: Information Security Policies, Standards, and Processes:
http://hhcinsider.nychhc.org/corpoffices/EITS/Pages/Information-Security.aspx.

- Access Control Policy
- Asset Management Policy
- Authority to Establish Enterprise IT Information Security Policies
- Bring Your Own Device Policy
- Business Continuity and Disaster Recovery Policy
- Communications and Operation Management Policy
- Data Encryption Policy
- Incident Management Policy
- Information Security Risk Management Policy
- Overarching Information Security Policy
- Physical and Environmental Security Policy
- Security Compliance Policy
- Security Policy on Cloud Computing Services
- Vendor Management Policy
- Cybersecurity Incident Response Plan
- Information Security Program Plan
- Physical and Environmental Security Plan
- Systems and Communication Plan
- Vulnerability Management Plan
- Bring Your Own Device Standard
- Cloud Computing Security Standard
- Data Encryption Standard
- Log Management Standard
- Device and Media Control Standard
- Password and Access Code Standard
- Information Security Glossary

10. External Security Standards & References:

- COBIT5_AP007: Manage Human Resources
- NIST SP800-53: Security and Privacy Controls
- NIST SP800-53: Managing IS Security Risk
- NYS Policy_NYS-P14-001: *Acceptable Use of Information Technology Resources*
- NYC_DoITT: *User Responsibilities Policy*
- NYC Policy: *Limited Personal Use of City Office and Technology Resources*

11. Review & Authorization:

Authored By:

Enterprise IT, ISRM-GRC Service Line

Reviewed By:

- The Information Security Policy Steering Committee on 01/11/22. The Committee is comprised of:
  - Chief Corporate Compliance Officer, Senior Assistant Vice President or appointed delegate(s)
  - Human Resources Vice President or appointed delegate(s)
  - Office of Legal Affairs Senior Vice President or appointed delegate(s)
  - MetroPlus Health Plan President & CEO or appointed delegate(s)
  - Enterprise IT Senior Vice President or appointed delegate(s)
  - Enterprise IT ISRM Service Line
- Enterprise IT Senior Leadership: 12/02/21

Approved By:

Soma Bhaduri, Assistant Vice President, Chief Information Security Officer & Information Security Policy Steering Committee Chair

Soma Bhaduri Digitally signed by Soma Bhaduri Date: 2022.04.06 10:40:39 -04'00' 4/6/22

Signature Date

Authorized By:

Kim Mendez, Senior Vice President, Chief Information Officer

Kim Mendez Digitally signed by Kim Mendez Date: 2022.04.07 14:49:37 -04'00' 4/7/2022

Signature Date

12. Revision History

Date	Description of Change	Reviewer
03/31/17	• Added statements to ensure alignment with The City of New York Policy on Limited Personal Use of City Office and Technology Resources released in June of 2016 • Added PHI definition • Updated user responsibilities to include privacy reporting requirements and reporting of incidents to Inspector General • Updated Information Security Policies link • Updated list of related ISRM: Information Security Policies and Standards	Enterprise IT Leadership & ISPSC
04/26/18	• 4.0-Definitions: Workforce Member definition revised pursuant to OCC request and approval by ISPSC. • 4.0-Definitions: POMD definition from BYOD Policy has been included. • 4.0-Definitions: Management definition added • 5.0-Policy Statement: Entire section reformatted to align with current policy format. • 5.0-Policy Statement: Section 2.0 concerning direct reference to BYOD Policy added under B. Information Technology Devices. • 6.0-Workforce Member Responsibilities: Email address for the Corporate Privacy and Security Officer has been updated.	Enterprise IT Leadership & ISPSC
10/29/19	• Personal Device and System Business Contact definitions revised and added to align with the ISRM-BYOD Policy. • User: Definition revised to clarify connection between terms 'Workforce Members' and 'Users'. • 5.F: Revised to align with related statements present in the ISRM- BYOD Policy, • Updated HIPAA Security OP (250 Series) references.	Enterprise IT Leadership & ISPSC
10/15/20	• *Data Classification* definition revised • *Policy Statement* revised to emphasize change in environment, i.e., augmented number of telecommuters • Statement 5.D.2.e revised slightly per OCC feedback to align with COI OP language • 5.G.3.e added to align with language in BYOD Policy	Enterprise IT Leadership & ISPSC
06/01/21	• Revised Personal Device definition to align with change in BYOD Policy (replaced IT resource with device). • 5.F: Revised to reflect changes in the Enterprise IT and OCC environment resulting from an increase in Telecommuter Workforce. • Added statement 5.5 to align Access Control Policy changes • Added definitions for Port Forwarding and Router to support above referenced statement addition. • Added reference to OP 20-62: Telecommuting	Enterprise IT Leadership & ISPSC
11/15/21	• Section 5F: Added statements #4 and #5 to address recurrent incidents of inappropriate use of non-NYC H+H email use to conduct business on behalf of the System.	Enterprise IT Leadership & ISPSC

Questions concerning this Policy
may be submitted to the ISRM Service Line at*:*
ISRM-GRC@nychhc.org

(Continued on Next Page)

NYC
HEALTH+
HOSPITALS

Information Technology Resources Acceptable Use Policy

Workforce Member Acknowledgement Page

____

I hereby attest that I have read and comprehend the policy statements set forth in the System's *Enterprise IT-ISRM: Information Technology Resources Acceptable Use Policy*. Furthermore, I understand that my signature below certifies that I am aware of and agree to comply with the following requirements:

- All NYC Health + Hospitals Workforce Members are required to maintain the confidentiality of the System's IT resources.
- Workforce Members may not use the System's IT resources for unlawful purposes.
- The System's IT resources may not be used for any purpose, or in any manner that may prove detrimental to the health system, its Patients, Workforce Members, and its interests.
- Limited personal use of the System's IT resources may not interfere with access to or use of the System's IT resources for official purposes, may not hinder productivity, patient care, or prevent other Workforce Members from performing their official job duties.

Finally, I understand that violation of any of the policy statements communicated in the System's *Enterprise IT-ISRM: Information Technology Resource Acceptable Use Policy* may result in disciplinary action up to and including termination.

Workforce Member (Print Name): ____

____ ____________________

Signature Date