NYC HEALTH+ HOSPITALS

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

Effective Date: March 15, 2016

Review Frequency: Annually

Revised: November 28, 2018

Document Reference:
NYC Health + Hospitals_EITS_ISRM_Policy_002.3

NYC HEALTH+ HOSPITALS

1. Goal

NYC Health + Hospitals (the System) provides Workforce Members with access to numerous information technology (IT) resources (PCs, laptop, information systems, electronic data, etc.). Acceptable organizational use of IT resources and effective security requires the participation and support of all Workforce Members. Unacceptable use of IT resources exposes the System, Workforce Members and patients to potential risks. The objective of this Policy is to identify the System's acceptable use standards that shall be implemented in conjunction with the acceptable use standards outlined in the System's *Privacy and Security Operating Procedures.*

2. Scope & Applicability

The scope of this Policy includes all System 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 10).

3. Policy Authority

The NYC Health + Hospitals Chief Information Officer (CIO) has the authority to oversee, direct and coordinate the establishment and implementation of IT policies, standards, and guidelines for the System.

4. Definitions

IT Resource: 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).

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: employees, volunteers, trainees, interns, and members of NYC Health + Hospitals Board of Directors.

User: Workforce Member that has been authorized and has been granted access to IT resources.

Protected Health Information (PHI): Refers to any information, including demographic information collected from an individual and genetic information, whether oral or recorded in any form or medium, created or received by NYC Health +Hospitals 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. PHI is classified as *restricted data*.

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

NYC HEALTH+ HOSPITALS

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

Personally Owned Mobile Device (POMD): For the purpose of this Policy a personally owned mobile device refers to a mobile computing device that was not purchased or issued to the workforce member by the System. POMDs include: laptops, smart phones, tablets, and portable storage devices (external hard drives, USB thumb drives, etc.).

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.

5. Policy Statement

Workforce Members shall follow these user requirements and information security controls when accessing the System's IT resources:

A. Access Control

1. Unauthorized access to, storage of, disclosure or transmission of, and alteration or destruction of 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:
        i. 250-17: HIPAA Security Policy - Integrity
        ii. 250-19: HIPAA Security Policy - Transmission Security
    b. Enterprise Information Technology Services (EITS), Information Security & Risk Management (ISRM): Access Control Policy
2. 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.
3. Enterprise Information Technology Services (EITS) shall create, amend, or disable Workforce Member access to IT resources only when requested and authorized by Human Resources (HR) or Management.
4. 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 *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, 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, access, store, receive, 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 health system's IT resources *is permitted* 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 (i.e., 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' Policy.
   b. knowingly or recklessly 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. may interfere with, or causes a disruption to, the health system's IT resources,
   d. is for the purpose of gaining unauthorized access to other IT resources,
   e. is deemed as inappropriate, or offensive behavior/activity in the workplace; and
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 are to be submitted to Management.
5. Limited personal use of the health system's IT resources is at the sole risk of the Workforce Member. The health system is not responsible for any loss or damage resulting from such personal use.

E. Information Technology Resources

1. The following user requirements and information security controls apply to the use of **System owned and/or issued IT resources**:
   a. System data that is accessed, created, stored, transmitted or received is the property of NYC Health + Hospitals.
   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 *Security Configuration Standard.*
   e. Altering the security configuration settings of IT devices is strictly prohibited.
   f. Removal of IT devices from NYC Health + Hospitals facilities requires Management approval.
   g. Disposal or reallocation of IT devices by anyone other than EITS Team Members is strictly prohibited.
   h. Upon termination of employment or affiliation with NYC Health + Hospitals, all IT devices issued to a user must be returned to Management or Human Resources.

2. The user requirements and information security controls applicable to the use of the System's authorized personally owned mobile devices are defined in the *EITS-ISRM: Bring Your Own Device (BYOD) Policy.*

F. Email

1. Access to NYC Health + Hospitals email system is granted to Workforce Members for the purpose of conducting the official business of NYC Health + Hospitals.
2. Use of NYC Health + Hospitals email system to send chain letters, e-mail spam, inappropriate messages, or unapproved newsletters and broadcast messages is prohibited.
3. Sending the health system's restricted or private data to a non-NYC Health + Hospitals' email account or domain requires Compliance approval. Once allowed, email must be encrypted per the *EITS-ISRM: Data Encryption Standard.*
4. Users shall exercise caution when clicking on links and/or opening attachments within emails.

G. 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(s), including Internet storage sites, which may harm or be inconsistent with the System's policies, practices, and goals.
3. Use of cloud computing services shall comply with the System's:
    - *EITS-ISRM: Security Policy on Cloud Computing Services*
    - *EITS-ISRM: Cloud Computing Security Standard*

H. Software

1. Downloading unauthorized software onto IT resources is prohibited.
2. Only software approved or managed by NYC Health + Hospitals Enterprise Information Technology Services (EITS) Department may be installed on IT resources.
3. Unauthorized duplication of NYC Health + Hospitals software is strictly prohibited and is subject to civil and criminal penalties.

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

1. Disclosure of the System's proprietary, confidential, sensitive, or identifying patient information 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 unless explicitly approved by Management.
3. Workforce Members must comply with *the NYC Health + Hospitals 20-61: Social Media Use Operating Procedure* at all times.

NYC HEALTH+ HOSPITALS

6. Workforce Member Responsibilities

All Workforce Members are required to:

1. Complete required training, which may include, but may not be limited to: *HIPAA Privacy & Security General Workforce Training*, *Information Security Awareness Training*, and specific information system user training as required.
2. Contact the Enterprise Service Desk (ESD) at EnterpriseServiceDesk@nychhc.org, or by phone at 877-934-8442 immediately to report **confirmed or suspected information 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.
3. 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 On Privacy-Related Complaints to The Facility*. Questions related to this Policy or referenced Operating Procedure may be directed to your supervisor, your Facility's Compliance Officer, or to the Corporate Privacy and Security Officer at CPO@nychhc.org.
4. 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.*
5. Read and abide by the referenced *NYC Health + Hospitals Operating Procedures, EITS-ISRM: Information Security Policies,* and *EITS-ISRM: Information Security Standards.*
6. Comply with all NYC Health + Hospitals Policies and Operating Procedures.

7. Exceptions

In the event that adherence to this Policy is not feasible, an *ISRM Policy Exception Request* must be submitted to ESD. The request must include a business justification and a detailed description of the compensatory security measures that will be employed to mitigate potential security risks. *Policy Exception Requests* shall be reviewed by the Corporate Chief Information Security Officer (CISO) or designee. The CISO's designee shall maintain a record of approved *Policy 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.

NYC HEALTH+ HOSPITALS

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 (select 250 HIPAA PnP)

- 20-58: Information Systems Application Access Policy & Procedure
- 20-60: Limited Personal Use of HCC Office and Technology Resources
- 20-61: Social Media Use
- 250-01: Security Management Process
- 250-05: HIPAA Security Policy-Workstation Use
- 250-06: HIPAA Security Policy-Information Access Management
- 250-08: HIPAA Security Policy-Workforce Security
- 250-17: HIPAA Security Policy-Integrity
- 250-18: HIPAA Security Policy-Person & Entity Authentication
- 250-19: HIPAA Security Policy-Transmission Security
- 250-20: HIPAA Security Policy-Remote Use & Access To Electronic Protected Health Information

ISRM: Information Security Policies, Standards & Related Documents:

http://hhcinsider.nychhc.org/corpoffices/EITS/Pages/Information-Security.aspx.

- NYC Health + Hospitals EITS–ISRM: Authority to Establish EITS Information Security Policies
- NYC Health + Hospitals EITS-ISRM: Access Control Policy
- NYC Health + Hospitals EITS-ISRM: Asset Management Policy
- NYC Health + Hospitals EITS-ISRM: Bring Your Own Device Policy
- NYC Health + Hospitals EITS-ISRM: Incident Management Policy
- NYC Health + Hospitals EITS-ISRM: Information System Acquisition, Software Development and Maintenance Policy
- NYC Health + Hospitals EITS-ISRM: IT Resources Acceptable Use Policy
- NYC Health + Hospitals EITS-ISRM: Information Security Risk Management Policy
- NYC Health + Hospitals EITS-ISRM: Overarching Information Security Policy
- NYC Health + Hospitals EITS-ISRM: Security Policy on Cloud Computing Services
- NYC Health + Hospitals EITS-ISRM: Vendor Management Policy
- NYC Health + Hospitals EITS-ISRM: Password and Access Code Standard
- NYC Health + Hospitals EITS-ISRM: Incident Response Standard
- NYC Health + Hospitals EITS-ISRM: Cloud Computing Security Standard
- NYC Health + Hospitals EITS-ISRM: Information Security Policies & Standards Glossary

NYC HEALTH+ HOSPITALS

10. External Security Standards & References:

- 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*
- COBIT5_AP007: Manage Human Resources
- NIST.SP.800.53: Security and Privacy Controls
- NIST.SP.800.53: Managing IS Security Risk

11. Review & Authorization:

Revised By:
EITS-ISRM Service Line

Reviewed By:

- The Information Security Policy Steering Committee on 04/17/18. 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)
  - EITS Senior Vice President or appointed delegate(s)
  - EITS-ISRM Service Line
- EITS Leadership: 11/28/18

Approved By:
Krisha Neighbors, Interim Information Security Policy Steering Committee Chair, Senior Director, ISRM

Signature _____ Date 12-7-18

Authorized By:
Kevin Lynch, Senior Vice President, Chief Information Officer

Signature _____ Date 12/7/18

NYC HEALTH+ HOSPITALS

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	EITS 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.	EITS Leadership & ISPSC
11/28/18	• 5.F.2: Adjusted language to include Compliance approval	EITS Leadership

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

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 *EITS-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.
- 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 *EITS-ISRM: Information Technology Resource Acceptable Use Policy* may result in disciplinary action up to and including termination.

Workforce Member (Print Name): _____

_____ _____

Signature Date