NYC
HEALTH+
HOSPITALS

Enterprise Information Technology Services Information Security & Risk Management: Security Policy on Cloud Computing Services

Effective Date: May 1, 2017

Review Frequency: Annually

Revised: February 19, 2019

Document Reference:
NYC Health + Hospitals_EITS_ISRM_Policy_008.2

1. Goal

Cloud computing technology provides numerous benefits to organizations, including scalability, high performance, less administrative overhead, cost efficiency, agility, flexibility, and new innovation opportunities. However, without adequate security controls, the implementation of cloud technology can expose NYC Health + Hospitals (the System) to numerous risks that may threaten the confidentiality, integrity and availability of the System's information technology (IT) resources. Understanding, managing and controlling these risks is crucial to ensuring that the implementation of cloud computing services does not compromise the security of the System's IT resources.

The goal of this Policy is to communicate the security controls that shall be implemented to ensure that cloud computing services are implemented in a manner that complies with applicable federal, state, and local laws and regulations and with applicable NYC Health + Hospitals Privacy and Information Security Policies.

2. Scope & Applicability

From a technology perspective, the scope of this policy includes, but is not limited to, the following cloud computing services and deployment models:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Private Cloud Model
- Community Cloud Model
- Public Cloud Model
- Hybrid Cloud Model

Specifically, this Policy applies to the System's Workforce Members who are Information Owners, IT Resource Administrators, or Workforce Members whose role involves identifying, recommending, requesting, implementing, or managing IT resources and/or technology solutions that may involve cloud computing services or related technology components. Information security is the responsibility of all Workforce Members. While not all Workforce Members will be directly impacted by the requirements set forth in this Policy, all Workforce Members are required to be aware of and to comply with any element of the Policy that may apply to them.

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 (EITS) policies, standards, and guidelines for the System.

4. Definitions

Cloud: Refers to a term used for global networks; originally used to reference the telephone network, now commonly used as a reference to the Internet

Cloud Computing: The practice of using a network of remote servers hosted on the Internet (In an External Site) to store, manage, and process data.

Cloud Computing Service: Is a service provided by a third party to offer fully managed easy, scalable access to applications, resources and services.

Cloud Infrastructure: Is the collection of hardware and components, such as servers, storage, network, and virtualization software needed to support a cloud computing model.

Cloud Service Provider (CSP): Refers to an entity that provides cloud based services.

Cloud Access Security Broker (CASB): Refers to a particular set of cloud security solutions that provide an integral layer of cloud cybersecurity centering around four main pillars: visibility, compliance, data security, and threat protection.

Cloud Computing Service Models:

- *Software as a Service (SaaS):* In this model the cloud service provider's application runs on a cloud infrastructure and is accessible by the consumer online via a web interface or via a desktop application. The consumer has no control over the underlying hardware configuration.

- *Platform as a Service (PaaS).* Via this model the consumer of the cloud service deploys or installs onto the cloud infrastructure a consumer-created or acquired application. The application must use programming languages, libraries, services, and tools supported by the cloud service provider. The consumer has no control over the underlying hardware configuration, storage, network, operating system or management layers.

- *Infrastructure as a Service (IaaS):* With this model the consumer utilizes the cloud service provider's processing and storage facilities, their network, and other computing resources. The consumer is able to install and run any software, which may include operating systems and applications. While the consumer does not have any control over the underlying cloud infrastructure, it has control over operating systems, storage, and deployed applications.

Cloud Computing Deployment Models:

- *Private Cloud:* The cloud infrastructure is commissioned for exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. Also may exist in or outside the country.
- *Community Cloud:* The cloud infrastructure is commissioned for exclusive use by a specific community/sector of consumers from organizations that have shared nature of work and obligations. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. Also may exist in or outside the country.
- *Public Cloud:* The cloud infrastructure is commissioned for open use by any organization. It may be owned, managed, and operated by a private or public organizations or a combination of them. It exists on the premises of the cloud service provider.
- *Hybrid cloud:* The cloud infrastructure is a composition of two or more different cloud infrastructures (private, community, or public) that remain separate entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., load balancing between clouds).

Data Classification: Data classification requires that data be categorized according to sensitivity level and degree of impact to the System should the data be disclosed, altered or destroyed without 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. The unauthorized disclosure, alteration or destruction of this type of data could cause a *high level of risk*. Examples: PII (Personally Identifiable Information), which includes, Social Security Numbers (SSN), date of birth, payment card cardholder data, protected health information (PHI), financial information, employee data, etc. The highest level of security controls should be applied to this type of data.

2. ***Private Data (Moderate Sensitivity)***: Data is classified as private when the confidentiality of the data is preferred due to its moderate sensitivity level. Examples: Physical plant detail, information security plans, meeting minutes, budgets, etc. Unauthorized disclosure, alteration or destruction of private data could result in a *moderate level of risk*. 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*. Examples of public data include press releases, research publications, list of services provided, company directories, etc. 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.

Information Owner: Also referred to as *Asset Owner,* pertains to the Business Unit or Department that is operationally responsible for the information that IT resources transmit, process, or store.

Information Security Program: At a high-level, refers to the policies, processes, and tools that are necessary to prevent, detect, document and counter security threats to digital and non-digital data. In sum, a security program defines the framework required for maintaining a desired security level. This policy is a crucial element of NYC Health + Hospitals Information Security Program.

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).

IT Resource Administrator: Also referred to as *Asset Custodian,* is an EITS Workforce Member who is responsible for the management and maintenance of enterprise IT resources.

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).

Protected Health Information (PHI): Protected Health Information (PHI) means 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 NYC Health + Hospitals 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*.

User: NYC Health + Hospitals Workforce Member who has been authorized to access and has been granted such access to the System's IT resources.

Workforce Member: 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.

5. Policy

The following outlines the security controls that shall be applied and the organizational requirements that shall be accounted for when planning, reviewing, negotiating, and initiating a cloud service outsourcing arrangement.

1. Cloud service requests shall be reviewed and managed by EITS.
2. EITS will seek to implement cloud specific security technologies and processes, such as CASB solutions, when feasible.
3. EITS shall rely on the *NYC DoITT Policy: Citywide Policy on Cloud* for guidance as necessary.
4. Cloud service requests that involve restricted data require the approval of Management and Office of Corporate Compliance.
5. CSPs under consideration must demonstrate the ability to comply with the various laws and regulations that are applicable to the health system.
6. CSPs under consideration must demonstrate the ability to support the System's records management program requirements.
7. CSPs that will have access to restricted and private data must comply with the provisions set forth in the System's *EITS-Information Security & Risk Management (ISRM): Vendor Management Policy* and the System's *Business Associate Agreement* when applicable
8. CSPs under consideration shall undergo the *NYC Health + Hospitals Vendor Information Security Risk Assessment Questionnaire* prior to the signing of a service contract.
9. CSPs under consideration must demonstrate compliance with applicable security controls identified in *NYC Health + Hospitals Cloud Service Standard* and applicable EITS-ISRM: Information Security Policies. These controls may include, but may not be limited to:

    A. Access Control

    1. Required identity and access management policies, practices, and technologies to ensure authorization, secure authentication, role-based access, auditable access, and timely access termination.
    2. Access control policy and procedures that support the System's *EITS-ISRM: Access Control Policy,* the *EITS-ISRM: Password and Access Code Standard*, and OP 250-16: HIPAA Security Policy Access and Authentication Procedures.

    B. Asset Management

    1. Asset management policies and procedures that supports the System's *EITS-ISRM: Asset Management Policy.*
    2. Evidence of an implemented Bring Your Own Device (BYOD) Policy and personal device use management procedures.
    3. Policies and procedures that address data inventory, data flow, data classification, data labelling, and data handling (including disposal).

C. Business Continuity

1. Business continuity and data availability policies and procedures that support the System's required data availability, data backup, data recovery, data retention and disaster recovery service levels.
2. Physical and environmental security to ensure that data center utilities are in optimal condition, secure, safeguarded against risks, monitored, maintained, redundant, and are regularly tested.

D. Data Protection

1. Application & Interface Security to ensure that applications and programming applications and interfaces are designed, developed, deployed, and tested in accordance with the System's standards and adhere to applicable legal, statutory, or regulatory compliance obligations.
2. Data integrity controls (including policies and procedures) to ensure data input and output integrity routines (i.e., reconciliation and edit checks) have been implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.
3. Required data protection policies and procedures, including, but not limited to, encryption, penetration testing, vulnerability management, malicious code execution and data management solutions employed to ensure controlled access to data, to secure data while at rest, in transit and in use.
4. Documented baseline of security configurations that are implemented along with documentation that demonstrates annual testing of same.
5. Required physical and logical architecture and configurations to safeguard against unauthorized access of, intentional, or unintentional alteration of IT resources.
6. Demonstrated ability to provide structured and unstructured data in the System's standard format upon request.

E. Incident Management

1. Incident management policy and procedures that support the System's *EITS-ISRM: Incident Management Policy* and *Incident Response Standard,* including evidence of forensic procedures that support the System's requirements for the presentation of evidence to support discovery of potential legal action after a security incident.

F. Information Security Management

1. Evidence that demonstrates the implementation of an Information Security Management Program.
2. Evidence of documented control framework that is reviewed at least annually.

G. Risk Management & Compliance

1. Risk Management practices that comply with the System's *EITS-ISRM: Risk Management Policy*.
2. Audit assurance and compliance to ensure that audit plans, with a focus on reviewing the effectiveness of implemented security operations, have been developed and maintained in order to address business process disruptions.
3. Demonstrated audit assurance and compliance supported via independent audits that are performed at least annually.

H. Service Delivery

1. IT governance and service management practices that meet the System's standards.
2. Change control and configuration management policies and procedures that meet the System's standards

I. Personnel Security

1. Implementation of an Acceptable Use Policy that supports the System's *EITS-ISRM: Information Technology Resources Acceptable Use Policy.*
2. Personnel screening practices that support the System's practices.
3. Personnel separation practices that support the System's practices.

4. Evidence of a sanction policy for workforce members who have violated security policies and procedures.

10. Personnel privacy and security awareness training that supports the goals of the System's Privacy and Security Awareness Program.
11. CSPs shall be subject to, at a minimum, annual NYC Health + Hospitals managed information security risk assessments and shall be responsible for mitigating identified risks.
12. CSP contractual requirements and service level agreements shall be explicitly recorded in the service agreement and shall include contractual obligations that must be observed upon termination.
13. CSP performance shall be continuously assessed by Information Owner and EITS to ensure contractual obligations are being met.

6. Workforce 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 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 Information Security & Risk Management Department via email at CISO@nychhc.org.
2. Report incidents related to **unauthorized acquisition, access, use or disclosure of PHI** must be reported 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 Privacy 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 Standards (see *section 9*) upon gaining access to the NYC Health + Hospitals Intranet and completing required HIPAA Privacy & Security Training and applicable Security Awareness Training,
5. Comply with all NYC Health + Hospitals Policy 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, and the CPSO. 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.

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

- 50-01: Corporate Compliance and Ethics Program
- 120-19: Corporate Records Management Program and Guidelines for Corporate Record Retention and Disposal
- 250-01 to 250-21: HIPAA Security Policies

ISRM: Information Security Policies, Standards, and Processes:

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

- EITS-ISRM: Access Control Policy
- EITS-ISRM: Asset Management Policy
- EITS-ISRM: Authority to Establish EITS Information Security Policies
- EITS-ISRM: Data Encryption Policy
- EITS-ISRM: Bring Your Own Device Policy
- EITS-ISRM: Incident Management Policy
- EITS-ISRM: Information System Acquisition, Software Development and Maintenance Policy
- EITS-ISRM: Information Security Risk Management Policy
- EITS-ISRM: Information Security Risk Management Policy
- EITS-ISRM: Information Technology Resources Acceptable Use Policy
- EITS-ISRM: Overarching Information Security Policy
- EITS-ISRM: Physical and Environment Policy
- EITS-ISRM: Cloud Computing Security Standard
- EITS-ISRM: Data Encryption Standard
- EITS-ISRM: Incident Response Standard
- EITS-ISRM: Password and Access Code Standard
- EITS-ISRM: Information Security Policies & Standards Glossary

10. External Security Standards & References:

- NYC DoITT Policy: Citywide Policy on Cloud
- COBIT 5_APO13: Manage Security
- NIST.SP.800-53
- Cloud Security Alliance Cloud Controls Matrix v3.0.1

11. Review & Authorization

Authored By:

EITS-ISRM Service Line

Reviewed By:

- The Information Security Policy Steering Committee on 01/15/19. 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 Leadership: 02/04/19

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

Signature ______________________ 2-14-19
Date

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

Signature ______________________ 2/19/19
Date

12. Revision History

Date	Description of Change	Reviewer
12/18/18	• 2.0 Scope and Applicability: Revised to reflect current standard of distinguishing between direct and indirect Workforce applicability. • 9.0 Related OPs and ISRM Policies & Standards: Updated to reflect current list. • 11.0 Review & Authorization: Updated to reflect review period and current EITS Leadership.	EITS Leadership & ISPSC

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