HEALTHQUEST

Title: Physical and Environmental Policy	Type/Number: *HQ 5.7*
Effective Date: December 1st, 2015	Owner: *CISO, HQ IT*

For use at:

☒ HQ System, Inc (**ALL**)	☐ The Thompson House	☐ Northern Dutchess Hospital
☐ HQ Medical Practice	☐ Health Quest Urgent Care	☐ Putnam Hospital Center
☐ Health Quest Heart Center	☐ Health Quest Home Care	☐ Vassar Brother Medical Center
		☐ Other:

POLICY

The Physical and Environmental policy provides direction to effectively manage the locations at which Health Quest's information assets that are stored and satisfy the operating requirements of the business and clinical needs. This policy includes but is not be limited to the design, implementation and overall management of the physical and environmental controls and procedures as it regards the protection of information assets including the data it houses.

The overall goal of the policy is to ensure that following are managed effectively:

- Facilities access and monitoring controls
- Contingencies Operations
- Access controls, authorizations, and monitoring procedures
- Maintenance Records
- Repairs and modifications

PROCEDURES

1.1 Physical Safeguards

Health Quest IT, in conjunction with HQ Security and Facility Operations, will apply effective and efficient controls to secure the locations at which technical devices are stored in order to minimize the risk of vulnerability to its information assets. In addition, Health Quest employs reasonable safeguards at each of the locations at which such IS assets resides to protect against natural and environmental hazards, events, and potential risk, as well as guarding against unauthorized access and intrusions.

Health Quest's manages the environment in a manner that minimizes risk to the physical environment, the systems and data within the location, and the environmental and access control mechanisms in place to ensure that the risk of threats and vulnerabilities are minimized. These threats and vulnerabilities include:

- Unauthorized Physical access (internal or external)
- Risk of natural or man-made disasters (flooding, fire, terrorism, structural damage)
- Penetration or denial of service attacks
- Social Engineer into the data facility or physical location

- Loss of data (due to environmental control e.g., electro static, humidity)

The development and maintenance of this policy is the responsibility of the CISO.

1.2 Physical Access Controls

HQ Facilities Management and Security in conjunction with HQIT, assesses the risks and defines and implements procedures that limit the physical access to its information assets and the facilities in which they are housed. All access to such assets is to be properly authorized.

This policy is owned by the CISO. Deploying appropriate measures to effectively secure information assets is the shared responsibility of the CISO, CSO and CIO.

The Physical access control mechanisms should be identified and documented. They include, but are not limited to:

- Door locks
- Electronic access control systems
- Security officers
- Video monitoring
- Manual access logs
- Warning signs
- Alarms

1.3 Contingency Operation Plan

Health Quest's contingency operations policy ensures that there are procedures in place for the continuation of business operations and or restoration of data following significant interruptions in business and IT operations.

Prior to an emergency situation, Health Quest will ensure that physical and environmental security can be maintained with the use of mitigating controls during the period that operations are disrupted. These mitigating controls may include:

- Use of security guards
- Transfer of services to a remote site
- The ability to manage fire/flooding/structural damage to the building
- Procedures to re-enter the building in the event of a disaster
- Integrating the physical contingency plan with the Business Continuity Process or Disaster Recovery plans

1.4 Facility Security Plan

Health Quest facility security plans document the use of physical access controls and will ensure that each facility has the safeguards to protect the facility and the equipment stored within it from unauthorized access, tampering and theft.

The facility security plan should be in response to a risk assessment and analysis that will document access levels and the roles which require that level of access e.g. Public, patients, visitors, escorted, business partners and staff. The physical access controls that need to be documented include, but are not exclusive to:

- Locked doors (and their control systems), restrictive area warning signs, surveillance cameras and alarms
- Property controls such as asset tagging
- Personnel controls – different Identification badges for staff, contractors, escorts, visitors, maintenance
- Access logs where appropriate
- Security services and continuous monitoring (guard or patrol)

1.5 Access Control and Validation Procedures

Health Quest has defined procedures for access controls and validation. These procedures include physical access to the facility based on an individual's role with monitoring and periodic review of access records.

The procedures are designed to validate user's access to each physical location based on the user's role or job description. In addition, the procedures should indicate those who are authorized to have access to the access control systems software.

Periodic recertification of access to sensitive physical locations e.g. computer rooms is required at a minimum of 12 months.

Changes to a users' access need to be authorized, documented and auditable.

1.6 Maintenance Records

In order for Health Quest to have full visibility of and ensure a continuous business operation there must be provision and resource available for appropriate maintenance to take place within the facility.

Health Quest must have procedures in place to ensure that all maintenance activity is logged and documented. If accesses to restricted areas are by external contractors or maintenance staff is required they will be accompanied and escorted during the duration of the visit by a member of the IT staff with the appropriate access. In addition, if the area contains sensitive data, the individual (unless covered by a blanket agreement with 3rd party vendor) must sign or must have signed a non-disclosure agreement (NDA), Business Associate Agreement (BAA) or equivalent for external contractors.

REFERENCES/SOURCES

HIPAA		**ISO 27001:2005**	
Title	**Number**	**Title**	**Number**
Facility access control	§ 164.310(a)(1)	Securing offices, rooms and facilities	A.9.1.3
Contingency operations	§ 164.310(a)(2)(i)	Protecting against external and environmental threats	A.9.1.5
Facility security plan	§ 164.310(a)(2)(ii)	Equipment sitting and protection	A.9.2.1
Access control and validation procedures	§ 164.310(a)(2)(iii)	Supporting utilities	A.9.2.2
Maintenance records	§ 164.310(a)(2)(iv)	Equipment maintenance	A.9.2.4
Contingency operations	§ 164.310(a)(2)(i)	Physical security perimeter	A.9.1.1
		Protecting against external and environmental threats	A.9.1.4

POLICY HISTORY:

Supersedes: All previous Physical and Environmental Policies
Date Reviewed: 11/20/2015
Date Revised: 11/21/2015