HEALTHQUEST

Title: Data Protection Policy	Type/Number: *HQ 5.9*
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

This policy forms the foundations upon which Health Quest manages the confidentiality, availability and integrity of its information and data assets while in transmission and at rest.

Health Quest management will ensure that following are managed effectively:

- All Health Quest data is classified in accordance with the Security Management policy
- Data flow analyses which are performed to ascertain where controls are required to protect data according to its classification
- Data transmission
- Data storage
- Encryption and decryption
- Data backup and recovery
- Data destruction

PROCEDURES

1.1 Data Classification

Health Quest IT (HQIT) is responsible for the storage and distribution of all data for which it is the custodian.

In order for HQIT to effectively manage and ensure Health Quest's information assets, all employees and business associates must adhere to Health Quest Data Classification Standard and its Governance. This standard is maintained by the Office of HQ IT Security and its CISO are responsible for all employees being aware of it.

The office of HQ IT Security manages the program of data classification and governance throughout Health Quest and its covered entities to ensure that each information asset has an owner. While there are regulatory and industry standard definitions which will inform the classification of data and its governance the data owner has the final responsibility for classifying the data in their possession. The appropriate classification should be based on the following criterion:

- Value
- Legal, Regulatory, and Fiduciary Requirements

- Sensitivity to Patients, Clinicians and HQ as whole
- Criticality to the Health Quest

Health Quest's data will be classified in one of the following categories:

- Public
    - Data which can be shared with anyone requesting access to it. In many cases, public data are intended to be widely distributed (e.g., public health brochures and marketing materials). Inadvertent loss of such data poses no risk to the organization or its customers
- Internal or Company Confidential
    - Data which is meant to be shared only with those with a business need to know and, in most cases, with whom the organization has a relationship. This includes, but is not limited to employees, contractors and vendors. If these data were exposed to the public, they may cause harm to the organization or its customers but the release of the data are not prohibited by regulation.
- Sensitive/Confidential
    - Data which is meant to be shared only with those with a business or treatment related need to know. Electronic Protected Health Information as defined by HIPAA and consumer financial information as defined by PCI are both examples of this type of data. But it is not limited to those two definitions. Any data, the exposure of which could cause significant harm to Health Quest or its customers, should be classified as confidential.
- Confidential with limited distribution
    - These are data that should only be accessible to a very limited number of individuals. They include passwords, encryption keys, IP addresses and detailed system configuration information.

1.2 Data Flow Analysis

In order for Health Quest to manage its information assets there must be full awareness of the technical and logical environment in which it operates. An in depth documented flow analysis of the data that HQ either manages or communicates is maintained and reviewed periodically for accuracy. The analysis documents:

- All data stores and communication flows and will identify any areas of risk to Health Quest
- All information technology repositories of Health Quest data
- All data leaving Health Quest (either physically or logically)
- Any interaction with 3rd parties or external partners. All interaction with 3rd parties must be in accordance with the HQ Business Associates Agreement
- The information security controls in place to protect the data

The objective is to ensure that there are adequate physical, technical and logical controls in place to manage and maintain the security of HQ's information assets.

1.3 Least Privilege Access – Authorization

Access to Health Quest's data will be based on the following principles:

- Each user or system accessing HQ data or resources will be uniquely identifiable and authorized by HQ management
- The access policy will be followed at all times
- Data access is based on the principle of Least Privilege Access
- Any exception to the access policy will be documented and reviewed no less than annually

1.4 Data in Transmission

Data in transmission represents unique risks distinct from those of data at rest. Diligent and due care should be taken throughout the transmission process including the actual authorization of the transmission.

Below, the technical and logical protection measures that will ensure that electronically transmitted information is only modified with the appropriate authentication and authorization are described.

Sensitive data including any ePHI or PHI transmitted within the Health Quest network are to be encrypted when technically feasible.

When sensitive data are transmitted to an environment that is deemed external to Health Quest there will be technical control which ensure that the ePHI and PHI data are encrypted at a minimum of a AES 128 standard or + at point of exit and that the mechanism to decrypt the data are kept and managed in accordance to the Health Quest 3rd party policy, the Business associates agreement and regulation wherever appropriate.

Unencrypted transmission of confidential data outside the Health Quest intranet is prohibited by policy unless CISO has approved the use of other mitigating controls. This also will not apply if the transmission is mandated by a government agency which will not support an encrypted solution.

For the purpose of this policy, e-mail and movement of data to social media storage and "clouds" are considered an electronic transmission.

When data and/or information is transmitted physically (in the form of tapes, CD's, thumb drives, or other portable storage devices), they are to be encrypted. The data are to be shipped in tamper evident packaging and an inventory of what is shipped shall be maintained and secured by the shipper. Finally, receipt of such data shall always require a signature from the recipient.

1.5 Data at Rest

Health Quest ensures that there are appropriate controls in place to ensure the confidentiality of sensitive data when at rest. Data at rest can be defined as data which are stored on any of the following media (this is not a comprehensive list and is put here as examples):

- Storage drives e.g. computer hard drives
- Optical media e.g. floppy disks, tapes and compact discs
- Magnetic media e.g. Computer hard drives, tapes
- Hard copies of documents
- Removable media
- Social Media and Cloud Storage

Data at rest, regardless of the media on which it is stored including Cloud Storage, must adhere to the following criterion:

- For media storage, HQ IT Security must perform a security risk assessment of the requested storage media technology and approve such media prior to its usage.
    - Public "Cloud" Storage is not allowed (drop box, box, Google docs, etc.)
- Be used and available only on a need to know basis and be used at a minimum
- All access to it must adhere to the current "HQ access policy".
- Where deemed appropriate by the data owner, the classification of the data must be displayed to the viewer of the information. E.g. All non-public documentation must show the appropriate label, "Internal communication or sensitive, etc."
- Back-ups of the data must be as secure as the data itself unless documented differences are approved by the CISO.

Sensitive data stored within the Health Quest network are to be encrypted when technically feasible.

The CISO will develop data protection procedures if necessary which describe the minimum levels of protection needed when the data is "at rest".

When data which is persisted to a portable storage device is in transit, it will adhere to the standards for both data at rest and in transmission.

1.6 Encryption and Decryption

Encryption is an important mitigating control for data at rest and in transit.

All electronic PHI (ePHI) data must be encrypted when at rest when technically feasible. When ePHI is not stored encrypted, the reason must be documented with compensating controls that are approved by the CISO. For media containing ePHI, the information must be securely disposed or archived when no longer required in accordance to HQ data storage standards and applicable regulations.

Encryption keys will be managed within the IT department and will be accessible to the fewest possible individuals. If one of those individuals ever leaves the organization, the encryption keys must be changed as soon as feasible.

1.7 Integrity of Data Backups

Media and storage devices must be approved by Health Quest CISO before they can be used for storage of information assets. To ensure the integrity of backup data files, quality checks are and should be implemented (digital checksums, hash checking, etc.).

Before any data recovery process, the initial quality checks as mentioned above must be operable and agree before using it as restored data or the data request job will be re-initiated at point of failure and any data not passing the quality checks will be discarded.

After data recovery, the data quality checks will run again to ensure data integrity.

If there are any discrepancies in the verification of the data files' quality checks, an incident response and risk assessment must be conducted to determine if any further data contamination is present.

1.8 Data Destruction

Data shall be retained and destroyed in compliance with all applicable laws.

All data that are destroyed shall be assumed to be confidential. Therefore, all read/writable media are to be "zeroed" out with a degaussing mechanism or "zeroed" out using a Department of Defense compliant routine prior to disposing of the media.

Storage media are to be physically destroyed, shredded, and/or degaussed prior to disposing of the media and if a 3rd party is used they must be certified by a recognized industry standard and be accountable for the Storage media in transit and taken off site (via provide inventory reconciliation back to HQ IT) for destruction. In addition, the 3rd party must provide a certificate of destruction "COD" for each storage media data destruction performed.

Unless unavoidable, the destruction of data should take place using devices that are not connected to the Health Quest network.

REFERENCES/SOURCES

HIPAA		**ISO 27001:2005**	
Title	Number	Title	Number
Encryption & decryption	§ 164.312(a)(2)(iv)	Classification guidelines	A.7.2.1

Integrity	§ 164.312(c)(1)	Information labeling and handling	A.7.2.2
Mechanism to authenticate electronic protected health information	§ 164.312(c)(2)	Network controls	A.10.6.1
Transmission security	§ 164.312(e)(1)	Information handling procedures	A.10.7.3
Integrity controls	§164.312(e)(1)(i)	Protection of organizational records	A.15.1.3
Encryption	§164.312(e)(1)(ii)	Data protection and privacy of personal information	A.15.1.4
Data backup and storage	§ 164.310(d)(2)(iv)		
Data backup plan	§ 164.308(a)(7)(ii)(A)		
Disaster recovery plan	§ 164.308(a)(7)(ii)(B)		

POLICY HISTORY:

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