HEALTHQUEST

Title: Access Policy	Type/Number: 1
Effective Date: December 1st, 2015	Owner: *CISO,HQ IT*

For use at:

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

POLICY

Adequate, appropriate and secure access controls and user access management should be applied to control access to Health Quest's information systems and information technology infrastructure components. The goal is to ensure authorized user access and prevent any unauthorized access to and/or improper use of Health Quest information systems and information technology infrastructure components. The "least privilege" access model is to be followed for all systems. Health Quest information systems are to be accessed only for uses approved by Health Quest. In general, this refers to members of the workforce accessing the information systems to perform the functions for which they were hired or otherwise affiliated with Health Quest.

PROCEDURE

Access control refers to the processes of managing a user's rights and privileges to access and perform functions using information systems, applications, programs, and files. The policy mitigates risk by restricting authorized users to access only the minimum information needed to perform job functions, including but not limited to:

- Authentication process
- Unique user identification
- Emergency access procedure
- Automatic logoff
- User account creation, revocation and suspension
- Review of user access rights
- Review of Separation of Duties
- Role-based access authorization management
- User password management

Account Creation / Authentication Process

Account creation refers to the processes involved in the initiation, approval and creation of user accounts on Health Quest information systems, as a result of events such as new employee hire or changes to an existing employee's functional role. Accounts are created with unique user names, ID's or numbers. When the process is manual, it should contain controls that, at a minimum, have ensure that:

- There is a document of the approval of account creation request by the Health Quest manager that has firsthand knowledge of the business need for such creation

- Ensure there is accountability for the management of an individual’s network (e.g. Active Directory) account to the current Health Quest manager or sponsor, who has firsthand knowledge of the individual’s functional role.

- Enforce use of the Online Universal Sign-on Request Form (hereafter, referred to as USRF) approved by Health Quest and provided in Health Quest’s Intranet, i.e. HQNet, when requesting for either new user account creation or for change of access rights of an existing user. The submission of USRF should be in accordance with the predefined Health Quest USRF submission procedure

- Create a record (e.g. system log entry) for each account creation that is sufficient for the purposes of auditing

Automated account creation through an Identity Management System is to follow approved business logic and is to be monitored and audited regularly for accuracy.

Account Disablement

When a user no longer has a business need to access an information system, then that access should be removed as soon as possible.

If an account is not in use, it should be disabled after 45 days of inactivity.

It is the responsibility of all Health Quest management to ensure that a user’s access to information assets is disabled as soon as is feasible. Access for terminated employees should be revoked as close to their termination as possible.

Account Suspension

Account suspension refers to the processes involved in the suspension of entitlements granted to an account.

An account may be suspended at the request of a user’s manager or as approved by a member of Health Quest senior management if there is reason to believe that that user’s access represents unacceptable risk to the organization.
Accounts are suspended instead of disabled when there is reason to believe that the account will be reinstated.

Health Quest’s account suspension processes should ensure documentation of the suspension request, timely analysis and remediation of suspended accounts, removal of suspended accounts and documentation of an audit trail for reinstatement of suspended accounts. An account may be suspended rather than disabled upon employment or contract termination if required by law or for forensic purposes.

Role-based Security Access Control
Permissions and privileges, (hereafter referred to as entitlements), for user accounts on Health Quest information systems are based on user's job roles and responsibilities and need to be managed appropriately and adequately. Role-based access control processes should contain controls that, at a minimum, have requirements to:

- Assign accountability for the management of the entitlements on Health Quest information systems, to a Health Quest Information Asset Owner, who has firsthand knowledge of the information system, and Health Quest Manager of the account holder who is in review. Entitlement Management includes all processes followed to authorize, modify, review, and revoke entitlements

- Maintain a record of all role-based access control matrixes which identifies the authorized access to Health Quest information systems

- Maintain a record of all users authorized to access the information system which identifies the unique user ID and the user's entitlements on that system

- Maintain a record of all modifications made to user entitlements which identifies the unique user ID and the nature of the modification (e.g. changes to permissions or privileges) if they are done on an individual basis. For example, over-riding an individual's role based access because they have a unique position that does not fit into the matrix.

Review of User Access Rights

User access rights of accounts and entitlements should be reviewed periodically to identify instances of inappropriate or excessive access to Health Quest's information systems by a user.

The user access review procedure should contain controls to ensure that reviews are conducted for accounts to determine if they are in contradiction of this policy or any Health Quest access standards. In the case of systems that are subject to an automated Identity Management system, periodic auditing of the systems business logic, including role based access control matrix, and verification that it is operating as designed replaces access review.

Access reviews will be performed on a quarterly basis by system administrators for each system.

Review of Separation of Duties

Periodic review of accounts and entitlements should be performed to identify instances of violation of principles of Separation of Duties (SOD) based on access rights authorized to a user in relation to access to Health Quest's information systems. Review of Separation of Duties processes should contain controls that, at a minimum, have requirements to ensure that processes are in compliance with regulatory requirements and Health Quest's Separation of Duties principles.

Where resource constraints make separation of duties unfeasible, management is to design, implement and document the use of other mitigating controls to lower the risk represented.

1.2 ACCESS CONTROL

Unique User Identification

User accounts should be unique and exclusive to a single individual, and they should comply with the security controls requirements prescribed in the Health Quest's user credential standard. Identity credentials will not be re-used after they are deleted from the Health Quest information systems.

- Initiate the process of mandating the provision of user's unique identifier, in conjunction with a secure password, to gain access to the requested access to Health Quest's information systems

- The use of shared accounts will be limited to systems where assignment of individual accounts is technically infeasible or where there are compensated controls in place, and these will be documented and will produce an audit record (e.g. user activity log) that is monitored for any inappropriate activity. Shared account credentials (e.g. User IDs and passwords) are subject to the same password rules as for an individual. In addition, the password must be changed when any individual sharing the account ceases the need for such access

- Passwords for individuals and groups should be changed every 90 days if not more frequently.

- Passwords for accounts with privileged access, e.g. Domain Administrators, should be changed every 60 days.

- The business case for shared accounts must be approved by the CISO.

- In the event that a system rather than an individual requires credentials (e.g., an application that needs to log on to a database), those credentials will be maintained by the application's user administrator. Those credentials are not to be used by individuals except as needed to trouble shoot a system error condition. The creation of the system ID, the date it was created and the business justification for it will be recorded in the HQ Risk Register.

- This policy explicitly prohibits circumventing user authentication or other security controls.

- When an individual's credentials are used to access a system, they are accountable for all system activity performed under those credentials unless they have notified the CISO that their credentials have been compromised.

Emergency Access

Emergency access refers to a procedure which results in person or a group of persons being given temporary and immediate access to a Health Quest information System in order to rectify an urgent patient care or business issue (e.g. repair a software malfunction). The control requirements are as follows:

- Emergency access controls should be established and documented to identify the types and instances of emergency situations

- Identify the accountable and required Health Quest managers, sponsors, technical resource and/or external entity needed to access Health Quest information systems during the predefined emergency situations. Accountable Health Quest managers or Sponsors are responsible for managing the defined emergency access processes during the emergency situations and the documentation of the event

- Emergency access should be removed within 30 minutes after the resolution of the emergency or when is feasible thereafter.

- The CISO must be notified via an e-mail whenever emergency access is granted. The e-mail should include the date and time of the change in privileges, when the privileges were removed, which credentials were impacted and a business justification for why the change was required.

Operating and Procedure Rooms

When providers are treating patients in operating rooms and procedure rooms and cannot physically access their electronic communication devices because of the nature of the procedure then it is permissible for the provider to grant proxy access for that device to another staff member in order to review urgent information necessary for patient care. Proxy access to the device can include sharing of the device password.

The following mitigating controls should be in place under these circumstances:

- The communication device will be password protected
- The device will be an approved device issued by Health Quest IT
- The passwords on devices intended to be used for this purpose will be changed no less frequently than every 30 days

- The device will have “remote wipe” capability

1.3 Remote Access

Health Quest must ensure that users (employees, business partners and vendors) are only provided with remote services that they have been specifically authorized to use.

Vendor remote access will be controlled so that their business need is reviewed regularly. The following mitigating controls will, at minimum, be in place for vendor remote access:

All vendor remote access will have a business sponsor who vouches for the business need for the access and that all necessary contracts and other agreements are in place before access is granted. The business sponsor notifies IT if the relationship with the vendor changes and access is no longer required.

- All Vendor remote access will be for a period of no more than one year. After that, the business sponsor of that access can request it be renewed for an additional year.
- Vendor remote access for the purpose of providing customer support is episodic. Once a ticket is open determining there is a problem, a vendor may be granted access. Once the problem is resolved, that vendor’s access is to be disabled.

1.4 Automated Identity Management

An automated identity management solution may be used in place of the processes described above so long as it provides the same level of control as the manual processes. Examples of such controls include but are not limited to:

- Manager confirmation of business need to know before granting access
- Suspension of access upon termination of employment
- Periodic review of user rights
- Role based access assignment where appropriate

REFERENCES/SOURCES

HIPAA		ISO 27001:2005	
Title	**Number**	**Title**	**Number**
Workstation security	§ 164.310(c)	Access control	A.11.1
Access authorization	§ 164.308(a)(4)(ii)(B)	User access management	A.11.2

Access establishment and modification	§ 164.308(a)(4)(ii)(C)	Application and information access control	A.11.6
Unique user identification	§ 164.312(a)(2)(i)	Cryptographic controls	A.12.3
Emergency access procedure	§ 164.312(a)(2)(ii)	Removal of access rights	A.8.3.3
Automatic logoff	§ 164.312(a)(2)(iii)	User identification and authentication	A.11.5.2
Access control	§ 164.312(a)(1)	Session time-out	A.11.5.5
		Limitation of connection time	A.11.5.6
		User authentication for external connections	A.11.4.2

POLICY HISTORY:

Supersedes: All previous Access Polices
Date Reviewed: 11/20/2015
Date Revised: 11/21/2015