One Health
Quality Alliance

May 2015

ONE HEALTH IT Security: Access Control Policy

One Health Quality Alliance

I. Purpose

The One Health Quality Alliance, LLC ("ONE HEALTH"), was formed as a limited liability organization, doing business as a clinically integrated physician-hospital organization. The members of the LLC as part of ONE HEALTH will help create value-based care in the region through health care services that control costs and ensure quality of care forth region.

To ensure secured and appropriate access to ONE HEALTH applications, systems and/or data used, processed, stored, maintained and/or transmitted in and through those systems. The policy defines individuals' responsibilities in promoting secured and appropriate access and applies to all ONE HEALTH systems.

II. Scope

This policy applies to employees, contractors, vendors, physicians, volunteers, board members, and business associates (ONE HEALTH Members). This policy applies to all existing applications and systems and to any new applications or systems acquired after the effective date of this policy

III. Policy

Users requesting access to applications, systems and data resources must follow accepted and prudent practices regarding computer security (see Data Handling & Exchange Policy).

ONE HEALTH employees identified as authorized by ONE HEALTH to grant access, must complete an IS Access Control Form for all users requesting/needing electronic access to systems or records. The form must be specific as to the access needed.

ONE HEALTH data and information stored on enterprise systems is considered confidential. Users must ensure that private and sensitive information is not disclosed to unauthorized individuals or organizations that do not have a legitimate reason for access to the information.

Completion of Computer Security Agreement

All staff members are required to read and sign the Computer Security Agreement before being provided with computer system access codes.

All staff members are required to complete annual training regarding privacy and security. Employees will be required to re-sign the Computer Security Agreement if any material changes are made to the agreement.

Users must only request access to official files and records necessary to perform duties as defined by the user's job description. Users must not request to access data or programs for which the user does not have authorization or explicit consent of the owner of the data.

No user actions can be performed on the information system without proper identification and authentication. Users are responsible for understanding and complying with all password use requirements including the need for adequate (difficult to decipher) passwords. Users are to use passwords of a mix of eight (8) alpha, numeric and special characters, with at least one uppercase letter, one lower case letter, and one number.

Users will be required to change their passwords every 90 days. Users must keep their passwords confidential and not share them with anyone.

It is the managers' or supervisors' responsibility to complete and Access Control Request for any change in a user's job function or employment that would require changes be made to the user's access at least five business day before such a status change. Managers and supervisors must specify both access to be added or revoked as appropriate for job changes. All data access will be periodically reviewed to ensure that the access remains appropriate.

Managers or supervisors must request that accounts or passwords for individuals who no longer require access to network resources be deactivated within 24 hours of user's change in status. On termination of employment, employees will have their access disabled. After a review by the manager or supervisor, the account may be subject to deletion. Managers and supervisors are responsible to ensure access is removed from any accounts to which the employee has access to that are not listed on the IS Access Control Form and/or for which PHNS does not control access to.

Users are responsible for reporting any suspected or actual computer access related incidents immediately to the Entity Chief Privacy & Security Officer, the ONE HEALTH Chief Privacy & Security Officer and the PHNS Compliance Specialist.

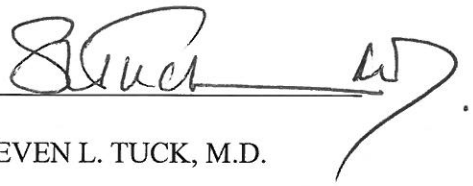
IV. Compliance

Failure to comply with any component of the Access Control Policy may result in

disciplinary action up to and including termination of employment. If an employee does not understand any part of the policy, it is their responsibility to obtain clarification from their manager or ONE HEALTH.

Adopted May 27, 2015

ONE HEALTH QUALITY ALLIANCE, LLC

By: 

Name: STEVEN L. TUCK, M.D.

Title: CHAIR