



One Health  
Quality Alliance

May 2015  
**ONE  
HEALTH  
IT Security:  
Data  
Handling &  
Exchange  
Policy**



## **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.

Data is information that supports the mission of ONE HEALTH. It is a vital asset and is owned or managed by ONE HEALTH. This policy establishes ONE HEALTH’s expectations regarding the handling and safeguarding of data. This policy is intended to ensure that the data is uniformly used and disclosed in accordance with all company policies and applicable local, state, and federal laws.

## **II. Scope**

This policy applies to employees, contractors, vendors, physicians, volunteers, board members, and business associates (ONE HEALTH Members). The policy applies to all data that is created, received, maintained/stored, transmitted, deleted and/or destroyed by ONE HEALTH.

## **III. General Information**

Users should be aware that the data they create on corporate systems or corporate applications remains the property of ONE HEALTH. Employees should note that any data and information on the systems will not be deemed personal or private. Employees are required to take reasonable steps to prevent unauthorized access to all data.

### **Definitions:**

**Authorized User:** Individuals who have been granted access to specific data assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include, but are not limited to employees, contractors, consultants, temporary employees, customers or other affiliates.

**Data:** Information that supports the mission of ONE HEALTH.

**Data Handling:** Using, storing, processing, transferring, administering, aggregating, sharing, and/or maintaining data.

**Electronic Messaging:** A set of communication processes used to relay data among the users of computers. Electronic Messages take many forms, i.e., Electronic Mail (E-Mail), FTP, text messaging, Instant Messaging and internet chat. **Encryption:** The process of encoding data so that it can only be read using the appropriate key/password and/or decryption algorithm

**External Data Sharing:** Restrictions on sharing of data outside of ONE HEALTH.

**Mail:** non-electric form, includes - U.S. Postal Service, DHL, UPS, FedEx, etc.

**Media:** All media on which data can be stored, either magnetically or optically, including, but not limited to: hard drives, magnetic tapes, diskettes, CDs, DVDs and USB storage devices.

**Mobile device:** Any electric and/or battery operated device that can be easily transported, and that has the capability for storing, processing and/or transmitting data, including but not limited to: laptops, tablets, mini hard drives, back-up hard drives, Zip Drives, Flash Drives, Personal Data Assistants (i.e. PDAs, including but not limited to Blackberries), Smart Phones, Hand Held/ pocket PCs, or any other mobile device designed or modified to store, process and/or transmit data.

**Physical Data Storage:** Physical devices that contain/store data. This includes, but is not limited to PC's, workstations, external hard drives, servers, CD/DVD, tape, USB Flash, laptops, and PDA's.

**Secure Transmission:** Transmissions whereby the data is encrypted and/or moved via protected means (i.e., VPN) so that it cannot be obtained or used by unauthorized parties.

#### **IV. Policy**

*Access:* Only authorized users will access, or attempt to access data. Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the data they access, and abide by applicable laws and policies with respect to accessing, using, deleting, destroying, or disclosing data. Notification of a user's termination or removal of authorized access to data must be conveyed as noted in the ONE HEALTH Access Control Policy.

*Collection:* Users should collect only the appropriate data required to perform company business. ONE HEALTH Management must ensure that all decisions regarding the collection and use of data are in compliance with the law and with ONE HEALTH policy and procedures.

*Controls:* Appropriate controls are required when handling, transmitting, storing,

deleting, or destroying data.

*Data Classification:* Authorization to access ONE HEALTH data varies according to its confidentiality or sensitivity (the need for care or caution in handling). For each classification, several data handling requirements are defined to appropriately safeguard the data.

It is important to understand that overall sensitivity of data encompasses not only its confidentiality (need for secrecy/privacy), but also the need to ensure integrity and availability. There are four classification levels that apply to data:

1. **Public:** Data intended for public use that, when used as intended, would have no adverse effect on operations, assets, obligations regarding privacy, or the reputation of ONE HEALTH or its patients.
2. **Internal:** Data not intended for parties outside of ONE HEALTH that, if disclosed, would have minimal or no adverse effect on the operations, assets, obligations regarding privacy, or the reputation of ONE HEALTH or its patients. Examples of Internal data include: policies and procedure, staff lists, and project data.
3. **Confidential/Restricted:** Data intended for limited use within ONE HEALTH that, if disclosed, could be expected to have a serious adverse effect on the operations, assets, obligations regarding privacy, or the reputation of ONE HEALTH or its patients. Examples of Confidential/Restricted data include: human resources, payroll, SSNs, financials, budgets, customer lists, employee health information, and credit card data.
4. **ONE HEALTH Confidential:** Data intended for use only within ONE HEALTH not to be viewed by any parties external to ONE HEALTH

Unless otherwise classified ONE HEALTH data is classified internal. ONE HEALTH Management will assess risks and threats to data under their control and accordingly classify the data where appropriate as *public*, *internal*, *confidential/restricted*, or *ONE HEALTH Confidential*. Data must be protected from unauthorized modification, destruction, or disclosure. ONE HEALTH Management must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect data. Employees must report instances in which data is at risk of or is aware of unauthorized modification, disclosure, or destruction occurring.

*Data Handling Requirements:* Example data classifications and the controls that must be used are listed below in the Data Handling Requirements Matrix. This list is not expected to be all inclusive, and questions about appropriate controls for data not

listed below should be directed to an immediate supervisor or manager.

Internal data and/or Confidential/Restricted data must not be taken off company property unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect the data. This data may not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.

Physical protection from theft, loss, or damage, must be utilized for all devices storing company data. When not directly in use, office, lab, and suite doors must be locked and any easily transportable/mobile devices (such as a laptop, PDA, or thumb drive) should be secured in locked cabinets or drawers. Physical protection also includes physical access controls (i.e., privacy screens) that limit physical access and viewing, if an area is open to public view.

Users of laptop and other mobile computing devices need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices at all times, but particularly when traveling, working away from the office, or outside of normal business hours. If not required to perform their work, employees must not save company data or customer PHI onto mobile devices. Mobile device users shall not process PHI data in public places.

Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.

Users must store company data (including documents, spreadsheets and data bases) that are created on a PC or similar system on a network drive to ensure proper security and backup.

Do not leave passwords, keys, or access badges for rooms or file cabinets containing company data in areas accessible to unauthorized personnel.

Store data recorded on paper documents in a locked drawer and/or in a locked room, or in another secure location.

*Data Retention and Disposal/Destruction:* Digital storage devices or media which contain licensed software programs and/or ONE HEALTH data must be destroyed or re-provisioned in accordance with the ONE HEALTH Asset Management Policy and/or vendor contracts.

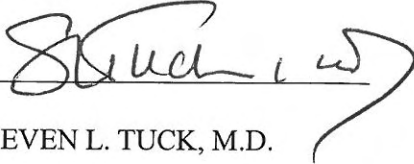
## **V. Compliance**

Failure to comply with any component of the Data Handling/Exchange Policy may result in disciplinary action up to and including termination of employment. If the ONE HEALTH Member does not understand any part of the policy, it is their responsibility

to obtain clarification from their manager or PHNS Inc.

Adopted May 27, 2015

**ONE HEALTH QUALITY ALLIANCE, LLC**

By: 

Name: STEVEN L. TUCK, M.D.

Title: CHAIR