UnityPoint Health

Title: File Sharing/Transfer 2.IT.16

Effective Date: 01/20

POLICY: All electronic files created, sent, or retrieved from or through the Iowa Health System, d/b/a UnityPoint Health ("UPH"), or used for UPH patient treatment, payment or operations ("TPO"), or research conducted at UPH affiliates, or any other business use are the property of UPH and its affiliates. Users of the UPH systems should have no expectation of or right to privacy in any type of file sharing/transfer. All use of file sharing and/or transfer must comply with the UPH file transfer procedures and rules.

DEFINITION: File sharing or transfer refers to movement of electronic data in a structured format (file) between two or more entities inside or outside the UPH network, referred to as file transfer in this policy.

SCOPE: System wide. All UPH affiliate facilities including, but not limited to, hospitals (see attached Addendum A), ambulatory surgery centers, home care programs, physician practices, all UPH and affiliate departments and covered group health plans, as applicable. References to UPH in this policy include UPH, its affiliates, and all organizations more than 50 percent controlled directly or indirectly by UPH. This Policy also applies to all external entities for which UPH provides file transfer services and personally-owned devices used to create, send, or retrieve UPH information.

This policy does not apply to routine transfer of files using the electronic mail system.

BACKGROUND: The purpose of this policy is to:

- protect UPH, its personnel, its customers, and its resources from the risks associated with the use of file transfers;
- define appropriate rules for secure use of file transfer systems, including access and use from home or other secure external locations;
- describe the expectations associated with the use of file transfer systems consistent with other UPH policies including, but not limited to, those prohibiting harassment and discrimination; and
- define UPH preferred tools to complete file transfers.

1. Definitions.

1.1 Cybersecurity (or Cyber Security). The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that are used to protect networks, computers, programs and data from attack, damage or unauthorized access.

POLICY RULES:

1. Purpose of File Transfers. The UPH file transfer systems and all electronic messages passing through or stored within the systems are the property of UPH and should be used primarily as a business tool to facilitate communications and to exchange information needed in the performance of job duties. The file transfer systems are to be used for legitimate business purposes only. Personal use of UPH file transfer systems is prohibited. UPH reserves the right to apply uniform and consistently enforced controls over its file transfer systems to the extent such controls are necessary to maintain production and discipline as permitted by law.

2. Corporate Standard. The corporate standard for business solutions requiring electronic transfer of files between UPH and third parties is secure file transfer protocol ("SFTP") and/or secure hypertext transfer protocol ("HTTPS"). All requests for secure FTP or secure HTTPS access through the corporate network must be approved by UPH security and compliance teams.

http://esp.ihs.org/ip/IP%20Public/Lists/Prepurcahse%20Security%20Review%20Requets/Interfaces%20and%20Interoperability.aspx

3. Approved Tools. UPH recognizes the need to have a consistent approved toolset to share/transfer files with third parties during normal business functions. All tools are required to comply with Policy, 1.IT.17 Encryption. UPH has approved the use of the following tools for file transfers/sharing.

3.1. MoveIT Transfer.

3.1.1. Used for ad-hoc (1 time or immediate need) transfers.

3.1.2. Active Directory integrated.

3.1.3. Allows for transfers within and outside the UPH network.

3.1.4. Audited periodically by UPH security and compliance teams.

3.1.4.1. Logs kept for 7 years.

3.2. Automate Enterprise.

3.2.1. Used for regularly scheduled, repeatable file transfers.

3.2.2. Hosted/supported by UPH Data Automation team.

3.2.3. Allows for transfers within and outside the UPH network.

3.2.4. Request for transfer should be made through UPH task management system (currently ServiceNow).

3.3. Microsoft OneDrive.

3.3.1. Used for internal file transfers with other UPH resources only.

3.3.2. Should not be used to share outside with UPH.

3.4. Teams/SharePoint.

3.4.1. Used for internal/external file sharing for specific needs.

3.4.2. Any access must be approved by internal UPH staff.

3.5. Box.com.

3.5.1. Currently allowed, but no new accounts will be created.

3.5.2. Will transition to MoveIT Transfer.

3.6. Legacy Tools.

3.6.1. Tools that exist at a site that is being newly integrated.

3.6.2. Site will provide list of tools.

3.6.2.1. Interoperability will review and recommend corporate standard tools.

3.6.3. Exceptions will be allowed on a case by case basis with approval of the security and compliance teams.

3.6.3.1. All exceptions will have an end date that defines when the exception will no longer be in use (within 1 year).

4. Unapproved Tools. No person shall install or attempt to install peer-to-peer file-sharing software on any company-owned computer. This rule informs all UPH employees, clients, customers that the use or installation of peer-to-peer ("P2P") file sharing or any other file sharing/transfer software not explicitly listed above on any network connected computer is strictly prohibited.

5. Third-party Computers (guests on the network). Any computer that connects to the UPH network must be free of file-sharing software. This rule allows the IT Department to scan computers belonging to third parties prior to allowing those computers to connect to the corporate network.

6. Monitoring. The IT Department will maintain controls on the corporate network to detect and block traffic from unauthorized file-sharing software.

7. Reporting. If you discover file sharing/transfer software on a company-owned computer, do not attempt to use it or to remove it. Users who discover unauthorized peer-to-peer file sharing software installed on a company-owned computer should immediately notify their managers or the IT Department.

8. Policy Violations.

8.1. Violations of this Policy may result in disciplinary actions at the department level, immediate revocation of system access and/or termination of employment or business contract.

8.2. Any suspected violations of this Policy should be reported to the appropriate management or affiliate compliance officer.

/s/ Kevin E. Vermeer

_____

Kevin E. Vermeer
UPH President

Addendum A: Legal Entity Operating Hospital

The entities listed below are accurate as of August 7, 2019. A current listing of legal named entities can be found at: http://https://uphealth.sharepoint.com/sites/intranet/policies/UPHandSystemwide/Addendum%20A.pdf

Region	Legal Entity Operating Hospital
CARTHAGE	MEMORIAL HOSPITAL ASSOCIATION
CEDAR RAPIDS	ST. LUKE'S METHODIST HOSPITAL
CEDAR RAPIDS	ST. LUKE'S/JONES REGIONAL MEDICAL CENTER
DES MOINES	UNITYPOINT HEALTH-DES MOINES
DES MOINES	GRINNELL REGIONAL MEDICAL CENTER
DUBUQUE	THE FINLEY HOSPITAL
FORT DODGE	TRINITY REGIONAL MEDICAL CENTER
KEOKUK	KEOKUK AREA HOSPITAL
PEORIA	METHODIST MEDICAL CENTER OF ILLINOIS
PEORIA	PEKIN MEMORIAL HOSPITAL
PEORIA	PROCTOR HOSPITAL
QC - MUSCATINE	UNITY HEALTHCARE
QUAD CITIES	TRINITY MEDICAL CENTER
SIOUX CITY	NORTHWEST IOWA HOSPITAL CORPORATION
WATERLOO	ALLEN MEMORIAL HOSPITAL CORPORATION
WATERLOO	UNITYPOINT HEALTH - MARSHALLTOWN
MADISON	MERITER HOSPITAL, INC.