From: Walton, Marty (HSC)
To: Walton, Marty (HSC)
Cc: Raines, Jill (HSC); Golden, Valerie (HSC); Milano, Mary L. (HSC); Nettleton, Sandra L (HSC)
Subject: HIPAA and Cloud Storage
Date: Tuesday, November 08, 2016 3:06:49 PM

Good afternoon, HCC Contacts, HCC Business Managers, HCC Researchers, and HCC Tier 1s/IT Representatives –

Please share the following reminder regarding **cloud storage** with the workforce members in your areas, including trainees, who store PHI of our patients or research participants:

HIPAA requires that all PHI be stored in a manner that protects the PHI from unauthorized access, and it prohibits making PHI accessible to individuals who are not authorized to access it.

-This specifically includes not sharing PHI with cloud storage vendors that are not approved by use by campus IT, such as Dropbox. (See approved products below.)

-Failing to protect PHI is a violation of HIPAA, as is sharing PHI with a vendor or putting PHI in a location where a vendor can access it, *unless IT has approved the vendor's product and appropriate contracts between the University and the vendor are in place*.

$$$ More than one health care entity has been fined several million dollars this year for HIPAA violations that included sharing PHI with a cloud storage vendor without having a BAA in place. $$$

Each campus IT department has designated an approved cloud storage product for PHI. Researchers and providers desiring to use cloud storage for PHI must use an IT-approved product.

1. Employees and trainees may contact their Tier 1, IT Representative, or IT Security for more information about their campus-specific IT- approved storage solution:

   Health Sciences Center –Sync & Share. See https://ouitservices.service-now.com/kb_view.do?sysparm_article=KB0010822 for information about Sync & Share. HSC employees and trainees also may store patient and research participant data on secure University servers or secure (encrypted) drives.

   Norman Campus - MS Office 365 (*after* the employee or trainee submits a request through IT Catalog for PHI storage within MS Office 365). Contact http://itscnorman.ou.edu/portfolio/security-consultation/. NC employees and trainees also may store patient and research participant data on secure University servers or secure (unencrypted) drives.

   Tulsa Campus HSC – SharePoint; network file shares, such as individual drives (U:); and departmental share drives (S:, T:, etc.).

   Tulsa Campus NC – Network file shares, such as individual drives (U:), and departmental share

drives (S:, T:, etc.).

2. If an employee or trainee wants to use an external storage vendor or cloud service provider for PHI, the employee or trainee must use a vendor or product approved by IT. **No PHI may be stored with cloud storage vendors that IT has not approved.**

Thank you for your assistance in ensuring that your workforce members, including trainees, receive this follow-up reminder to comply with these cloud storage requirements. I appreciate your help.

Jill Bush Raines
Assistant General Counsel, Office of Legal Counsel
and University Privacy Official
The University of Oklahoma
1000 S.L. Young Blvd., Room 221
Oklahoma City, OK 73117
(405) 271-2033
(405) 271-1076 (fax)
jill-raines@ouhsc.edu