Subject: HIPAA Penalty Update
Date: Thursday, July 28, 2016 5:23:28 PM

Good evening, Health Care Component Business Managers-

In just over 5 days, the Office for Civil Rights has announced HIPAA settlements with two academic medical centers totaling more than $5 million. The violations included the following:

-Storing PHI on unencrypted laptops/portable devices
-Storing PHI in the cloud without having a Business Associate Agreement in place with the cloud vendor
-Sharing passwords on systems that contained PHI
-Failing to implement physical security for devices that contained PHI

The two institutions, Oregon Health & Science University and the University of Mississippi Medical Center, paid $2.7M and $2.5M, respectively, to settle the allegations.

I want to make sure that all of you who are Health Care Component Business Managers are aware of the HIPAA settlements below because you are in a great position to help the University identify certain types of HIPAA issues in their areas.

For example, the $2.5M penalty against the University of Mississippi Medical Center was imposed for HIPAA violations that included unencrypted devices as well as for sharing PHI with vendors without having a Business Associate Agreement in place. *You may be aware of faculty or staff who use laptops that have not yet been encrypted or of vendor contracts that were not*

routed through Purchasing, meaning there is likely not a BAA associated with that vendor agreement. The $2.7M penalty against Oregon Health & Science University was for HIPAA violations that included unencrypted devices as well as storing PHI in the cloud without having a BAA in place with the cloud vendor. *If you know that employees in your area are using cloud storage, they need to contact Purchasing to ensure that the University has a BAA in place with the cloud vendor.* As a reminder, even if a contract for services is under the please-pay limit, if the services will involve the University's PHI, the contract must be routed through Purchasing so a BAA can be negotiated and put in place BEFORE any PHI is shared with the vendor.

Some actions you can take now to help protect your department's PHI:

-Ensure all agreements for vendor services that involve our PHI (e.g., collection, accreditation, storage) include a BAA. If you are not sure, please contact Purchasing.
-Remind employees to have your Tier 1/IT Representative encrypt devices that are used for University business, including simply checking email.
-If you are aware of shared passwords on medical equipment that stores PHI, such as ultrasound or x-ray equipment, ask your Tier 1/IT Rep to assign individual passwords.
-If you are aware of any medical equipment that is not physically secured, please find a way to secure it or contact me and we can discuss options.

Thank you for your help in protecting our patients', research participants', and health plan enrollees' PHI. If you have questions about the above or any other HIPAA issue, please contact me. *(If you are not a Business Manager of an HCC and would like to be removed from this list, please email me separately.)*

Jill Raines

Jill Bush Raines
Assistant General Counsel, Office of Legal Counsel
and University Privacy Official
The University of Oklahoma
1105 N. Stonewall Avenue, Suite 221
Oklahoma City, OK 73117-1221
(405) 271-2033
(405) 271-1076 (fax)
jill-raines@ouhsc.edu