

From: [Walton, Marty \(HSC\)](#)
To: [Walton, Marty \(HSC\)](#)
Cc: [Raines, Jill \(HSC\)](#); [Golden, Valerie \(HSC\)](#); [Nettleton, Sandra L \(HSC\)](#); [Milano, Mary L. \(HSC\)](#); [Duckett, Sally R \(HSC\)](#); [Engleking, Renee \(HSC\)](#); [Hogan, Donna F. \(HSC\)](#); [Smith, Sierra N.](#)
Subject: HIPAA Reminders for Researchers
Date: Friday, November 04, 2016 10:11:24 AM

Good morning –

Please share the following reminders with the workforce members in your area who work on human participant research projects that involve a treatment protocol. Information collected or created under the treatment protocol is likely Protected Health Information (PHI).

This year, the Office for Civil Rights has imposed more than \$20M in penalties against entities and individuals for HIPAA violations. Several of those penalties were imposed because researchers failed to protect research data that included PHI. Please review the following reminders and call me if you have any questions.

1. Some or all of your research data is PHI covered by HIPAA, so it must be protected just like clinical information is protected.
 - a. Secure documents when they will be unattended. Lock them in drawers or cabinets.
 - b. Do not share PHI with individuals or entities who are not authorized to have it. Your Informed Consent and HIPAA Authorization documents say who is authorized.
2. When sending PHI to the research sponsor or other researchers, you must use a secure transmission.
 - a. For faxes, use a fax cover sheet. Do NOT put PHI on the fax cover sheet.
 - b. For email, put the following in the subject line to secure the transmission: [secure] for HSC and [ouencrypt] for NC. (Use the brackets.)
3. Store PHI only on secure servers or encrypted devices. Do NOT store PHI on unencrypted laptops, local desktops, or unencrypted thumb drives.
 - a. Contact your Tier 1 or IT representative if you need help with identifying a secure server for your data.
 - b. Contact your Tier 1 or IT representative if you need to have your laptop or other device encrypted (including your personal devices).
4. Do NOT store PHI on a cloud unless you are POSITIVE that the University has a Business Associate Agreement with the vendor.
 - a. Putting PHI in an unencrypted cloud is a violation of federal law.
 - b. Putting PHI in a cloud without having a Business Associate Agreement in place is a violation of federal law.

- c. Ask your department manager or the Purchasing Department if a BAA is in place before you give *any* vendor any access to PHI.

Protecting research participants' PHI often requires an extra step or a minute or two more, but it is time well spent. Not only can that extra time protect the participants' information from unauthorized access, but it can also protect the University and its employees from fines and penalties. We want our participants to trust us with their information, and we can easily protect that information by taking the steps above. Thank you for your help in this important task.

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

CONFIDENTIALITY NOTICE: This email, which includes any files transmitted with it, contains confidential information from University Legal Counsel, is intended solely for the use of the individual or entity to whom it is addressed, and may contain information protected by the attorney-client privilege or work product doctrine. If you are not the intended recipient or the person responsible for delivering this email to the intended recipient, be advised that any use, dissemination, forwarding, printing, or copying of this email is strictly prohibited. If you have received this email in error, please notify the sender immediately by a "reply to sender only" message and destroy all electronic and hard copies of this email and any attached files.