NEW HIPAA RULES: HITECH ACT BREACH NOTIFICATION REQUIREMENTS TAKE EFFECT SEPTEMBER 23

Researchers who use protected health information in their research should be aware that the new HITECH Act breach notification requirements take effect on September 23, 2009. These requirements apply to “unsecured” protected health information (PHI) in electronic or paper form. Unsecured PHI is PHI that isn’t made unusable, unreadable or indecipherable to unauthorized individuals through the use of specific methods or technologies that have been approved by the Secretary of the Department of Health and Human Services (HHS Secretary). In general, this means that to be considered “secured,” PHI in electronic form must be encrypted. In addition, PHI in paper form must be destroyed at the time it is disposed.

If a researcher has unsecured PHI that is subject to unauthorized disclosure, use, acquisition or access, then the HITECH Act may require that the person whose information was compromised be notified of the breach. In general, notice will be required if the unauthorized disclosure, use, acquisition or access compromises the security or privacy of the protected health information by posing a significant risk of financial, reputational or other harm to the individual.

Notice of the breach generally must be given to the individuals involved by mail. If, however, the breach involves the PHI of ten or more individuals for whom the researcher doesn’t have sufficient contact information, then notice of the breach must be posted on the web or in “major print or broadcast media.” The notice also must be posted in print and broadcast media if the breach involves more than 500 residents of a state or jurisdiction, and the HHS Secretary must be notified in this case as well. The notice must be given as soon as reasonably possible, and in no event later than 60 calendar days after the breach is discovered, or should have been discovered.

The breach notification requirements do not apply to encrypted data. So to protect your data, be sure to talk to your IT personnel about encryption for your computers and accessories, especially your laptop and USB drive.

For more information on the HITECH requirements, contact the Office of Research Compliance at (404) 727-2398 or orc@emory.edu. For more information on encryption, see Emory’s new Disk Encryption Policy at http://policies.emory.edu/5.12 and Information Technology’s communication on Portable Computing Security Awareness at http://it.emory.edu/showdoc.cfm?docid=12429.