Subject: Another Large HIPAA Penalty Awarded

Good morning, all –

It's been a busy week for the Office for Civil Rights. Please read and share the brief report below that arose from a stolen laptop containing research participant PHI. OCR did not limit its investigation to encryption policies, however, and much of the $3.9 million penalty appears to be in response to the institution's failure to have procedures in place to inventory and track electronic PHI coming into and leaving its facilities. I'm taking this opportunity to remind you of three important steps you can take to protect your HCC:

1. Use the current onboarding and termination paperwork. Last summer, the University updated its new employee paperwork to address incoming PHI. It also updated its termination paperwork, including the Termination Checklist for all campuses and its termination letters (available on the HR website) for resignations, retirements, abandonment, and transfers. Please be sure you are using ALL of these documents EVERY time a member of your workforce – including residents and fellows – leaves your HCC. This is critical to the protection of the University's patient and participant PHI.

2. Maintain ePHI inventories. Jonathan Cox, our HIPAA Security Officer, is working with HCC contacts and Tier 1s to ensure your ePHI and device inventories are updated, as well as your procedures for checking out and tracking HCC-owned devices (laptops, flash drives, etc.) that contain PHI. He can help you if you need assistance with any of these processes. Jonathan-cox@ouhsc.edu.
3. Ensure that your electronic equipment acquisition practices comply with the University's policies. If the use will involve PHI, contact IT for a product review. When you contact the Purchasing Department to make the purchase, notify the buyer if the University's PHI will be involved, so the buyer can ensure that a Business Associate Agreement is included, when appropriate. (Recall that the P-card cannot be used for small dollar purchases for goods or services that involve PHI.)

If you have any questions about the employee forms or letters, please contact me. Thank you, again, for your work in the University's HIPAA compliance program.

March 17, 2016

Improper disclosure of research participants' protected health information results in $3.9 million HIPAA settlement

Feinstein Institute for Medical Research agreed to pay the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) $3.9 million to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules and will undertake a substantial corrective action plan to bring its operations into compliance. This case demonstrates OCR's commitment to promoting the privacy and security protections so critical to build and maintain trust in health research. Feinstein is a biomedical research institute that is organized as a New York not-for-profit corporation and is sponsored by Northwell Health, Inc., formerly known as North Shore Long Island Jewish Health System, a large health system headquartered in Manhasset, New York that is comprised of twenty one hospitals and over 450 patient facilities and physician practices.

OCR's investigation began after Feinstein filed a breach report indicating that on September 2, 2012, a laptop computer containing the electronic protected health information (ePHI) of approximately 13,000 patients and research participants was stolen from an employee's car. The ePHI stored in the laptop included the names of research participants, dates of birth, addresses, social security numbers, diagnoses, laboratory results, medications, and medical information relating to potential participation in a research study.

OCR's investigation discovered that Feinstein's security management process was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the entity. Further, Feinstein lacked policies and procedures for authorizing access to ePHI by its workforce members, failed to implement safeguards to restrict access to unauthorized users, and lacked policies and procedures to govern the receipt and removal of laptops that contained ePHI into and out of its facilities. For electronic equipment procured outside of Feinstein's standard acquisition process, Feinstein failed to implement proper mechanisms for safeguarding ePHI as required by the Security Rule.

"Research institutions subject to HIPAA must be held to the same compliance standards as all other HIPAA-covered entities," said OCR Director Jocelyn Samuels. "For individuals to trust in the research process and for patients to trust in those institutions, they must have some assurance that their information is kept private and secure."

The resolution agreement and corrective action plan may be found on the OCR website at https://urldefense.proofpoint.com/v2/url?u=http-3A__www.hhs.gov_hipaa_for-2Dprofessionals_compliance-2Denforcement_agreements_Feinstein_index.html&d=BQIFaQ&c=qRnFByZajCb3ogDwk-HidsbrxD-31vTsTBEIa6TCCEk&r=Uwzi50RQ7KVJAWE2DA3HmxgYBLC3wV3nwXD68IY8jsU&m=qz2MHYwQqNOwwCJLS8leq-

Ahv8qGMN_65ycEUNAnyyk&s=UtdlNbONvly5zgcRAbY_ThKdK-yx8r0D7pwFFKU3MLg&e= .