Subject: Oregon Health & Science University Agrees to Pay $2.7M to Settle 2013 Data Breaches
Date: Monday, July 18, 2016 9:08:32 AM

Good morning, all –

Please use this as a reminder to all faculty, staff, students, and trainees in your area of the following:

-PHI may not be stored in cloud computing systems unless you know that the University has a business associate agreement in place with that system. The University maintains secure data servers for the storage of PHI. Contact your Tier 1 or IT representative if you need help in determining where to store PHI.

-Laptops used for University business, including email, must be encrypted. Contact your Tier 1 or IT representative as soon as possible if you need to have your laptop encrypted.

Thank you for your help in protecting the University and its patients' PHI.

Oregon Health & Science University Agrees to Pay $2.7M to Settle 2013 Data Breaches

July 14, 2016

by Rajiv Leventhal

Oregon Health & Science University (OHSU) has signed a resolution agreement with the U.S. Department of Health and Human Services Office for Civil Rights (OCR) following an investigation of two data breaches of electronic protected health information (PHI) that occurred in 2013.

In one of the incidents, information of more than 3,000 patients at OHSU was compromised after medical residents inappropriately stored the data on a cloud computing system. The other incident that year involved a stolen [unencrypted] laptop containing the information of more than 4,000 patients. The resolution agreement just signed by the organization includes a one-time payment of $2.7 million and a rigorous three-year corrective action plan, according to an OHSU press release.

OHSU attests that no harm has been reported by any patients involved in either incident. Following an internal investigation in 2013, OHSU reported the breaches to OCR; offered free identity theft protection services to patients at risk for identity theft; established a 1-800-number to answer patient questions and concerns; implemented enhanced computer encryption across the university; and issued press releases outlining the incidents.

Over the next few months and beyond, OHSU integrity and information security experts will work with the consultant and the institution's steering committee to identify patient information security risks or vulnerabilities, and make regular reports to OCR, and implement any necessary mitigation strategies, officials say.

"Patient privacy has been and always will be a top priority at OHSU. OHSU is continuously working to improve protection of patient information data in a constantly changing security and technology landscape," said Bridget Barnes, OHSU CIO. "The two breaches that occurred in 2013 were stark reminders to OHSU how vigilant we must be. We made significant data security enhancements at the time of the incidents and now are investing at an unprecedented level in proactive measures to further safeguard patient information."

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