Subject: Learning from Others" Mistakes
Date: Tuesday, June 07, 2016 6:35:50 PM

Another good reminder of three important points:

-be sure your laptops, tablets, phones, and removable drives are encrypted

-store PHI (especially old PHI) on your HCC's secure server rather than a portable device

-destroy PHI you no longer need (See HIPAA News & Tips for destruction rules)

The recent theft of an unencrypted laptop that may contain information on up to 400,000 inmates who served time in California prisons has been added to the federal tally of health data breaches. Experts say notifying all those potentially affected could prove challenging.

The incident is the third largest breach added so far this year to the Department of Health and Human Services Office for Civil Rights' "wall of shame" tally of major health data breaches.

The laptop, which was stolen on Feb. 25, may have contained protected health information and personally identifiable information for patients within the California Department of Corrections and Rehabilitation who were incarcerated between 1996 and 2014, California Correctional Health Care Services says in a statement. The state agency has not yet verified what information was on the device, but it could have stored confidential medical, mental health and custodial information, the statement notes.

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