

From: [Golden, Valerie \(HSC\)](#)
To: [HCC Contact List](#); [HCC Business Managers](#)
Cc: [Raines, Jill \(HSC\)](#); [Walton, Marty \(HSC\)](#); [Milano, Mary L. \(HSC\)](#); [Nettleton, Sandra L \(HSC\)](#)
Subject: Storing PHI on Flash Drives?
Date: Tuesday, May 02, 2017 11:18:20 AM

Good morning, HCC Contacts and HCC Business Managers–

The notice below is a good reminder to take the important steps to use only encrypted flash drives to store PHI:

Western Health Screening, which provides onsite blood screening services at health fairs across the Colorado Western Slope region, is offering **15,326 affected individuals** protective services following a data breach. Much of the at-risk patient information is not highly sensitive—data on the drive included names, addresses and phone numbers, but some Social Security numbers also may have been compromised, said the healthcare organization.

The breach occurred when a **car owned by Western Health was stolen; a flash drive with the protected health information was in the car. The drive was password protected but not encrypted; it has not been recovered.**

Data on the flash drive can be accessed only by using a unique password, and to date, there is no evidence of data misuse, according to Western Health Screening. Still, the organization is offering three tiers of protective services from Kroll to affected individuals. The services being administered by Kroll include credit monitoring, identity theft restoration and fraud consultation, a service that other healthcare organizations have rarely provided after a breach incident.

If you have questions regarding these steps, please contact me, or your IT Tier One support. We're happy to help you take steps to reduce the risk of lost or stolen PHI!

Valerie Golden, RHIA
HIPAA Security Officer
Office of Compliance
The University of Oklahoma
(405)271-8001 x46456

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. 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.