COSMOS
Navigate the Compliance Universe

Compliance Today - November 2020
Enhancing privacy training for remote workers

By Donnetta Horseman

Donnetta Horseman (donnetta.horseman@moffitt.org) is Chief Compliance Officer at H. Lee Moffitt Cancer Center and Research Institute in Tampa, FL.

- linkedin.com/in/donnetta-horseman-193a388/

Is your privacy department experiencing an influx of privacy incidents related to an increase in remote workers? Consider updating your privacy training and distributing the following tips and reminders.

Device security and storage: Ensure employees are accessing your company's network according to policy and with the appropriate tools (i.e., a company-issued laptop and remote access applications and credentials.) If employees need to use a USB, flash drive, or any other removable storage device, ensure they are following policies and using encrypted devices. Employees should never use personal devices to store company-owned information. Patient information or confidential information should never be left unattended in a vehicle. It must be in the employee's possession and control at all times. This includes paper documents and any company-issued devices, including laptops, cell phones, or removable storage devices. Devices and patient or confidential information should be stored in a designated and secure private area at the remote work location. Employees, family, or friends should never use a company-owned device for personal reasons.