COSMOS
Navigate the Compliance Universe

Compliance Today - December 2022

Jan Elezian (jan.elezian@sunhawkconsulting.com) is a consultant and Director at SunHawk Consulting, LLC.

Privacy is paramount when working remotely in healthcare

by Jan Elezian, MS, RHIA, CHC, CHPS

As bad it was, the COVID-19 pandemic opened opportunities for workers to stay at home. Healthcare was not left out in the exodus to the home office. Coders and billers had already been remote for several years, thus giving healthcare organizations some advantage over other industries. Now, nonclinical staff—including finance, human resources, and IT—were ready to stick out the pandemic at home. Even clinical work such as primary care video visits and patient monitoring was now being accomplished remotely.[1]

Taking note in this shift, the U.S. Department of Health & Human Services was quick to publish guidance for healthcare organizations regarding cybersecurity while handling personal identifiable information (PII)/protected health information (PHI), and collaboration tools.[2] Paramount to a secure network is providing a virtual private network (VPN) to the home staff. The VPN creates an encryption "tunnel" that enables secure, end-to-end communications beyond traditional physical boundaries. The VPN must be patched timely and properly configured to protect confidentiality and prevent interception of data. Additional training for staff is needed regarding the use of the VPN, including two-factor authentication such as a token or a PIN number sent to a phone. Remote staff must secure the necessary modem and routers to facilitate the VPN. IT should ensure internet service with adequate bandwidth for the organization. Devices including computers whether enterprise-supplied or employees' "Bring Your Own Device" (BYOD), such as laptops, tablets, cellphones, etc., need to be secured to protect PII and PHI in all forms. Policies need to be developed to address acquisition, use, and maintenance of the mobile systems. Include in your policies or perhaps in a contract with the remote employee any BYOD and physical space requirements. It is recommended that at-home office space is dedicated, free of distractions, and not used for anything else. Office supplies may include a filing cabinet with a lock, a paper shredder, and a fire safe box for any PII/PHI to be stored at day end. The organization must ensure adequate staffing of the IT helpdesk to support increased remote staff.