# Compliance Today - September 2021
# How healthcare employers can avoid the legal perils of a remote workforce

By Dawn M. Irizarry, Esq., and Carolina A. Schwalbach, Esq.

**Dawn M. Irizarry** (dirizarry@cdflaborlaw.com) is Partner & Chair of the firm's Healthcare Practice Group, and **Carolina A. Schwalbach** (cschwalbach@cdflaborlaw.com) is Partner at CDF Labor Law LLP in Los Angeles, CA.

While the number of work-from-home and other remote work relationships has steadily increased over the years, the prevalence of these working relationships was kicked into overdrive early last year when the COVID-19 pandemic forced employers to immediately move their entire workforce to a remote platform. Unlike other service industries, prior to the pandemic, the healthcare industry had not embraced work-from-home and other remote working arrangements due to a variety of concerns; however, since then, all employers, including healthcare employers, have been forced to address these challenges in order to continue operations.

In this article, we will sort through the issues that arise in the healthcare setting when considering work-from-home and other remote work arrangements, including patient privacy issues, wage and hour concerns, and potential issues regarding workplace accommodations. In addition, this article will provide practical guidance regarding an employer's rights and responsibilities governing remote work arrangements.

## Patient protected health information

Healthcare employers face unique challenges when employees work remotely. In particular, healthcare employees need to access patients' protected health information (PHI) during the performance of their job duties. Federal, state, and local laws mandate that healthcare providers safeguard PHI from disclosure, including but not limited to the Health Insurance Portability and Accountability Act[1] and the California Confidentiality of Medical Information Act.[2] To comply with these legal obligations, healthcare employers must take specific measures to ensure that PHI is maintained as private when employees work remotely. Specifically, healthcare employers should do the following:

- Encrypt home wireless router traffic; properly configure, encrypt, and password-protect personal devices used by employees to access PHI while working from home (this includes firewall and antivirus protection);
- Change default passwords for wireless routers used;
- Encrypt all PHI before transmitting; and
- Require employees use a virtual private network when accessing the company intranet remotely.[3]

Healthcare employers would also be wise to develop and implement specific policies and procedures prohibiting employees from allowing friends or family from using devices containing PHI and mandating that their employees disconnect from the company network when they are not actively working. In addition, healthcare employers should consider providing employees who work from home and who regularly access PHI with locked file cabinets to store hard copies of documents containing PHI as well as Health Insurance Portability and

Accountability Act compliant shredders so they can destroy PHI once their work is complete.