AMA
AMERICAN MEDICAL ASSOCIATION

Private Practice Guide

Implementing a Work-From-Home Program

This guide, provided by the American Medical Association, helps private physician practices to identify and implement work-from-home positions for administrative staff. Implementation of work-from-home positions in health care has several benefits, including recruiting and retaining staff, being able to compete with other industries for talent, and limiting the number of staff members in the office to comply with social distancing guidance related to the ongoing COVID-19 pandemic.

Work-from-home benefits

- Social distancing compliance during potential virus surges
- Potential decrease in overhead (e.g., office space, parking)
- Improved employee satisfaction
- Support for colleagues in the office who may be experiencing burnout/fatigue
- Recruitment and retention advantage

Work-from-home programs can have many benefits, but it is important that the requirements are clearly defined and that the **security** and confidentiality of patient information are protected.

Tips for success

1. **Establish a clear purpose and define the scope of the policy.** The purpose and scope of this policy is vital to its success. A work-from-home policy for your practice should clearly establish why this policy exists, along with the benefits and cautions associated with it. It is recommended that a survey of current employees be conducted to determine their level of interest in working from home. Use survey results to implement what's best for your practice.
   a. **Specify what schedule of remote work will be allowed.** Will the practice implement a hybrid model in which employees spend specific days each week at home? Will some employees be fully remote, others on a hybrid model, and the rest always present on site?
   b. **Identify what types of remote work will be allowed.** Will all administrative staff work from home? Does this include billing and coding, transcription, prior authorization, and referrals? Will you divide each department into a mixed model so there is always someone from the department in the office while clinicians are seeing patients? What **steps** should be taken to ensure HIPAA compliance during remote work?
   c. **Establish if and how telehealth visits will be conducted by clinicians working remotely and monitor coverage and reimbursement outcomes.** Will you allow physicians, mid-level providers, and technicians to perform telehealth visits from home? Have you reviewed your payor contracts to ensure compliance with billing and visit locations? Have you reviewed insurance policies and Medicare coverage policies for telehealth visits? Many parity coverage policies continue through the ongoing Public Health Emergency. Check in with the AMA for the **latest federal guidance** to stay current.
2. **Outline a process.** Well-thought-out processes are as important to the success as the specifics of the work-from-home policy. A clear process should be outlined, reviewed, and tested prior to implementation across the practice. Feedback from staff in each department is especially useful during the review and testing period as what works for one department might not work for another, and several processes may need to be implemented to meet the needs of each area. Key questions to answer are:
   - What is the work-from-home schedule for staff by department?
   - How will remote staff connect with in-office staff on a regular basis?
   - How will sensitive data be transmitted from clinic to remote employees?
   - How will protected health information from telehealth visits be documented in the EHR from home in a secure manner?
   - What equipment is needed for employees to be fully functional from home?
   - How will telehealth visits be handled by clinicians working remotely?

Continued on next page.

3. **Outline expectations clearly.** A process is only as good as the communication that accompanies it. Make clear the operating hours of the practice to remote employees and the work to be completed within that timeframe. Depending on the type of work, flexible schedules may be possible. However, this should be evaluated independently, for everyone, and work dependencies between team members should be explicitly defined. Changes to a schedule—either temporary or permanent—should be discussed and cleared in advance with the office manager or practice administrator, and coverage should be secured before the changes go into effect.
    a. **Develop and implement a communication plan.** Scheduled **huddles** and/or audio/visual conferences for internal staff can reinforce collaboration among team members and ensure that important information is communicated in a timely manner.
4. **Set technology support and requirements.** For clinicians seeing patients remotely, identify the telehealth modality that is best for the practice. Synchronous telehealth, where the patient and clinician interact in real-time via telephone or audio-visual interaction via a smartphone, tablet, or computer, is the most used modality. Asynchronous telehealth via secure messaging in a patient portal, as well as remote patient monitoring, are also commonly utilized. The AMA has several **resources** available to physician practices related to telehealth and remote patient monitoring.
5. **Data and privacy considerations.** Securing private and confidential data is of the utmost importance, especially when working remotely. Health care data in any form must be held in a manner that helps to ensure its privacy and security. This includes physical and electronic controls. This **tip sheet**, created by the AMA, may help your practice keep its work environment safe from cybercriminals intending to disrupt your practice. Viruses, malware, and hackers can compromise both home and work **networks**, so it is important to stay diligent. For remote employees utilizing computers provided by the practice, follow this **checklist** to keep both your office and remote computers safe. As employees return to the office or you adopt a hybrid schedule, consult this **resource** to determine what additional technology considerations may be necessary for your practice. Your health IT vendor can also assist you with activating available privacy and security controls.
    a. **Computers, regardless of whether work-provided or personal devices, are susceptible to cyber-attacks.** Some common threats to stay vigilant against are *e-mail phishing* (an attempt to trick you into sharing private and confidential information through an email) and *ransomware* (malicious software that attempts to block the organization's access to its own information by encryption, with the end goal of obtaining money prior to releasing the information).
    b. **Consider using a Virtual Private Network (VPN).** VPNs provide a secure way to connect back to the office and access the practice management system, patient records, and images stored in the EHR.
    c. **There are additional considerations to take to secure your practice's information.** This includes the use of multifactor authentication, required and scheduled changes of passwords every 60–90 days (about three months), and the use of lock-out features for multiple incorrect log-in attempts.
    d. **Medical devices also create opportunities for cybersecurity intrusions to a physician practice**. It is important to establish formal processes of communication and coordination to identify and mitigate risks associated with medical devices. As these devices connect to hospitals and practices to share patient information, it is important to make sure medical devices are **cyber secure**.