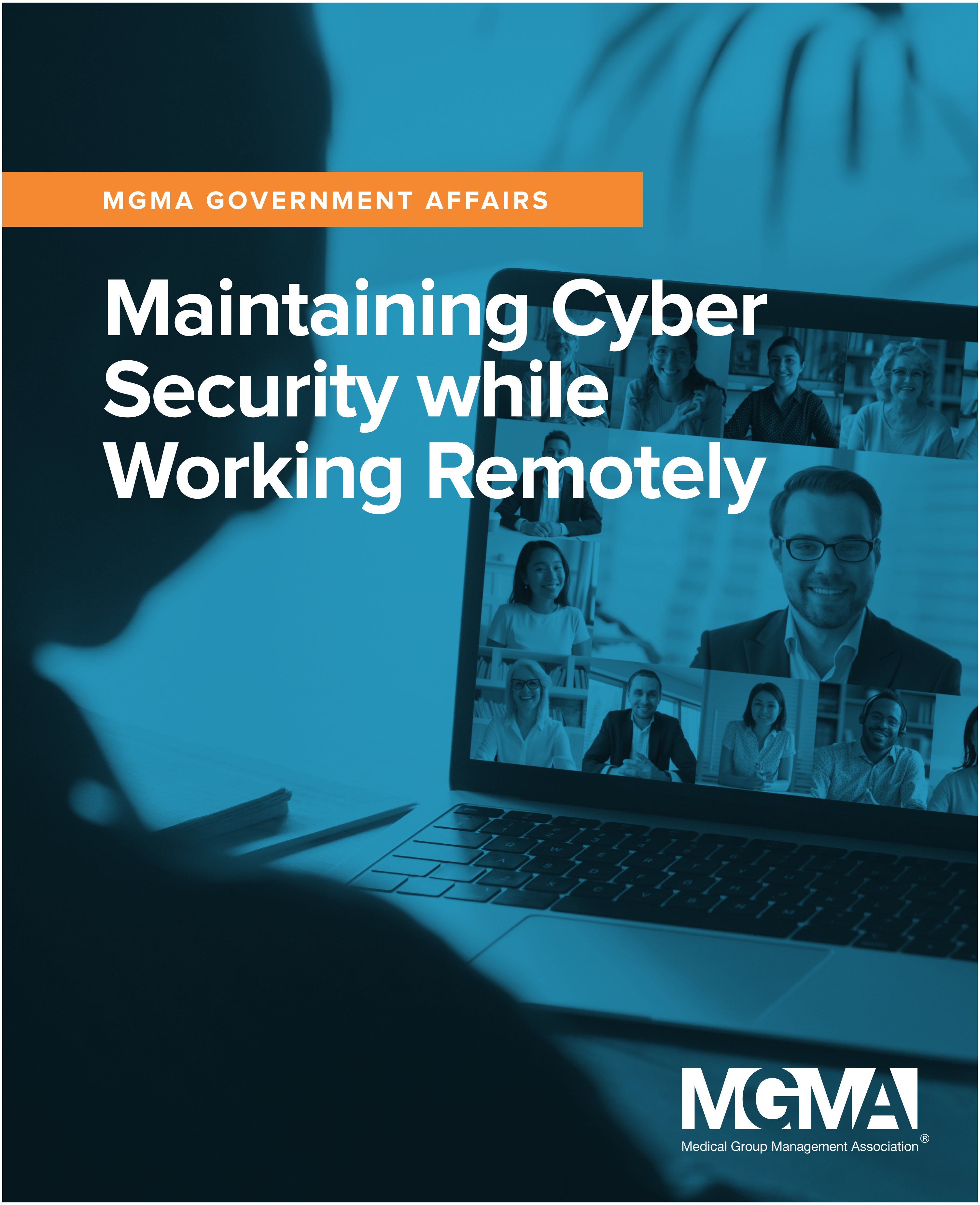

MGMA GOVERNMENT AFFAIRS

Maintaining Cyber Security while Working Remotely

MGMA
Medical Group Management Association®

CRITICAL THREAT AREAS

- Telehealth
- Ransomware attacks
- Loss of equipment/devices
- Vulnerable network
- Non-compliance with government requirements

Action Steps to Prevent Data Loss

1. **Create strong passwords.** Creating strong passwords (longer passwords that use a combination of letters, symbols, and numbers) will reduce the chance of a data breach caused by weak, reused or stolen passwords. Stronger passwords, however, are more difficult to remember. If you are storing these passwords for later recall, make sure to use caution when writing them down on paper or storing them in your phone or other device.

2. **Change your router login and password.** Change your router login and password. If you have never changed the router login and password, consider doing so. The default passwords for many models are not only too weak, but also known across the Internet and easily searchable. Attackers often simply write them into the code of malicious programs — if they work, the router is captured. Access the router settings to change the router username and password.

3. **Configure Wi-Fi encryption.** It is critical to configure your network connection correctly. Failure to do so may expose your network to cyberattack and the potential loss of patient information. Ensure that your connection is encrypted to keep information safe from prying eyes.

4. **Use a VPN if connecting to Wi-Fi networks that don’t belong to you.** Extra care should be taken if you are using an Internet connection not in your control such as Wi-Fi from a local business or your neighbor’s network. Public Wi-Fi networks are rarely encrypted and are susceptible to cyberattack. To prevent others connected to this Wi-Fi network from spying on you, consider employing a virtual private network (VPN). Typically, when connected through a VPN all of your data will be encrypted regardless of the network settings, and outsiders will not be able to read it.

5. **Secure your physical workspace.** Physical security should not take a back seat, even when you are working from home. Just as you lock your office when you leave for the day, do the same when working from home. Laptops can be stolen from your backyard, living room or home office. Take your laptop inside when you go and make lunch and make sure to lock the door to your home office. It is good practice to keep your home workspace as secure as you keep your normal office.

6. **Lock your device before walking away.** Someone can catch a glimpse of a patient record on your computer even when you are just having a cup of tea or taking a break so it is critical to lock the screen whenever you get up. Consider going into your computer settings and shortening the timeout intervals to reduce the chance that someone will view a record. Even if working at home with only family around you, locking your device is a good policy to avoid any issues.

7. **Do not leave your mobile devices accessible when taking them outside the home.** It is a best practice to keep work laptops and devices on your person at all times while out of your work environment. Avoid leaving devices on the car seat or even in the trunk of your car. As an additional precaution, consider employing encryption software to ensure patient information will not be accessible, even if a device is lost or stolen.

8. **Avoiding Internet speed-stealers.** Slow or spotty Internet service can impact your ability to effectively work remotely. To make the most of your high-speed Internet package, avoid programs that reduce your Internet speed such as streaming services like Netflix and Hulu. Visitors and family members using their devices on your Wi-Fi can also result in slower Internet speeds.

9. **Separate work and personal devices.** It is important to carve out boundaries between your work life and home life, especially while working from home. While it may seem cumbersome to constantly switch between devices to simple pay a bill or online shop, do your best to keep your work computer and home computer separate. Engaging in online commerce on your work device increases your chance of a cyberattack, so limit those activities to your personal devices.

10. **Backup your data.** To promote business continuity, avoid potential loss of revenue, and ensure access to patient information, it is critical to backup all your data. While external storage devices such as USB drives can be used, cloud-based storage services are preferable. If you use a mobile device management or enterprise mobility management service, then it is possible you will be able to initiate automated backups via your system's management console.

HIPAA ENFORCEMENT DISCRETION FOR TELEHEALTH

During the COVID-19 national emergency, practices and others subject to the HIPAA Rules are communicating with patients and providing services, through remote communications technologies (telehealth). Some of these technologies, and the manner in which they are used by practices, may not fully comply with the requirements of the HIPAA Rules.

The Office for Civil Rights (OCR), the federal agency responsible for enforcing privacy and security regulations issued under HIPAA, has announced that it will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against practices in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

Practices that want to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency can use any non-public facing remote communication product that is available to communicate with patients. OCR is exercising its enforcement discretion to not impose penalties for noncompliance with the HIPAA Rules in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency. This exercise of discretion applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19.

For example, a practice in the exercise of their professional judgement may request to examine a patient exhibiting COVID- 19 symptoms, using a video chat application connecting the provider's or patient's phone or desktop computer in order to assess a greater number of patients while limiting the risk of infection of other persons who would be exposed from an in-person consultation. Likewise, a covered health care provider may provide similar telehealth services in the exercise of their professional judgment to assess or treat any other medical condition, even if not related to COVID-19, such as a sprained ankle, dental consultation or psychological evaluation, or other conditions.

Under this Notice, practices may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency. Practices are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and practices should enable all available encryption and privacy modes when using such applications.

Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by practices.

Practices that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products. The list below includes some vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA.

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet
- Cisco Webex Meetings / Webex Teams
- Amazon Chime
- GoToMeeting
- Spruce Health Care Messenger

Under this Notice, however, OCR will not impose penalties against practices for the lack of a BAA with video communication vendors or any other noncompliance with the HIPAA Rules that relates to the good faith provision of telehealth services during the COVID-19 nationwide public health emergency.

MGMA Government Affairs

1717 Pennsylvania Ave. NW, #600, Washington, DC 20006
T 202.293.3450 | F 202.293.2787 | govaff@mgma.org

MGMA
Medical Group Management Association®