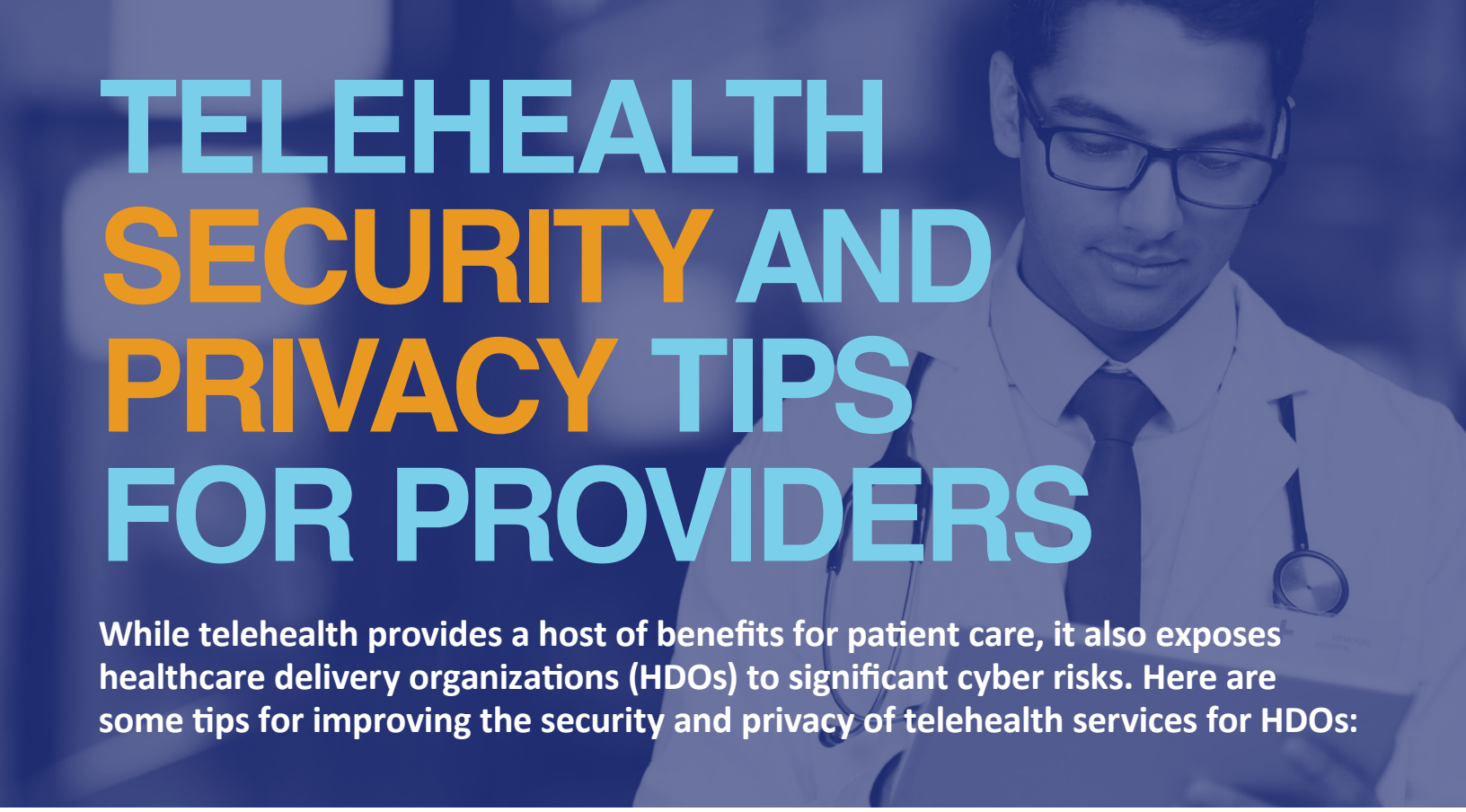


TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

While telehealth provides a host of benefits for patient care, it also exposes healthcare delivery organizations (HDOs) to significant cyber risks. Here are some tips for improving the security and privacy of telehealth services for HDOs:

SHARE UPDATED PRIVACY AND SECURITY PRACTICES WITH YOUR PATIENTS. Communicating privacy and security practices with your patients should be an integral part of your overall patient engagement strategy.

USE HIPAA-COMPLIANT APPLICATIONS to provide telehealth services when practical, and limit the number of applications used to help reduce security and privacy risks.

ENABLE ALL AVAILABLE ENCRYPTION AND PRIVACY MODES when using third-party applications for telehealth services.

MANAGE MOBILE DEVICE ACCESS. Isolate personal mobile devices from HDO applications, networks, and patient data. Corporate-owned devices should be granted the most access to HDO networks and information while personal mobile devices should have the least.

LIMIT NETWORK ACCESS. Apply defense in depth, network segmentation, and the principle of least privilege to prevent unauthorized access to patient information and medical devices.

USE MULTIFACTOR AUTHENTICATION WHENEVER POSSIBLE, especially when it comes to accessing your organization's most sensitive data.

MAINTAIN GOOD CYBER HYGIENE. Healthy habits for your information technology systems and applications will go a long way toward keeping them safe and secure. Run updates for equipment and applications as soon as they are available to take advantage of the latest security capabilities.

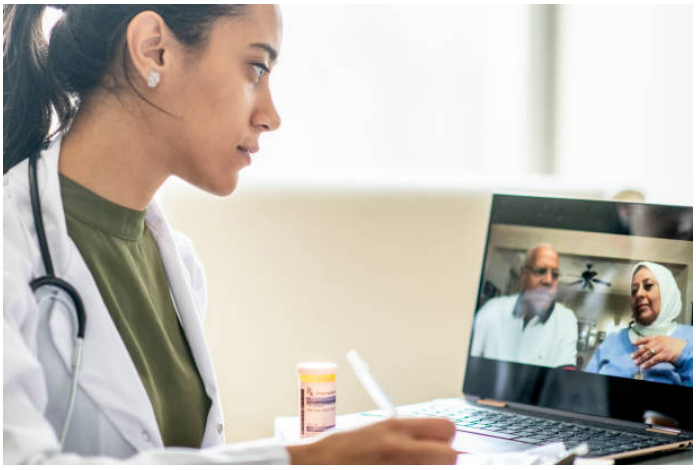
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST CYBER

TELEHEALTH SECURITY AND PRIVACY TIPS FOR PROVIDERS

During a telehealth visit, ensure your clinicians:

USE A PRIVATE SPACE and limit the number of people who take part in a telehealth session. Allow only personnel directly involved in the patient's care and individuals whom the patient permits to take part in a telehealth visit. Secure the room where you are conducting telehealth sessions (e.g., close the door and post a sign outside the door saying unauthorized individuals should not enter while your session is underway). Use headsets to limit others from hearing your patient and position screens out of the line of sight of others.



LIMIT THE INFORMATION REQUESTED to what is necessary to treat the patient.

SIGN OUT OF ALL APPLICATIONS and turn off all microphones, cameras, and monitors once the telehealth visit has concluded.

ADDITIONAL RESOURCES

Telehealth Security and Privacy Tips for Patients: https://www.nccoe.nist.gov/patient-tips

NCCoE Healthcare Sector Cybersecurity Guidance: https://www.nccoe.nist.gov/healthcare

NCCoE Mobile Device Security Guidance: https://www.nccoe.nist.gov/mobile

NCCoE Data Security Guidance: https://www.nccoe.nist.gov/projects/building-blocks/data-security

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST CYBER