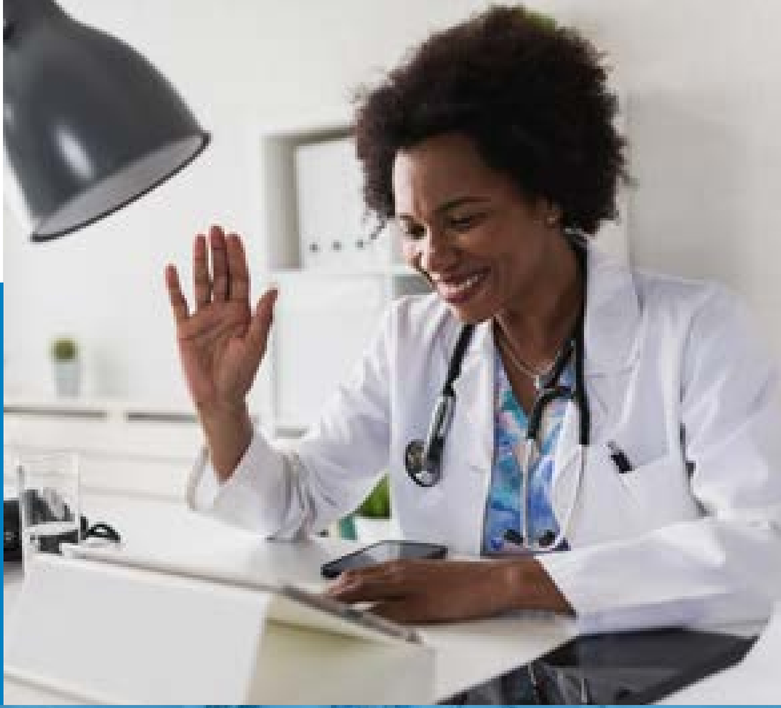
Ann & Robert H. Lurie
Children's Hospital of Chicago™
Children's Community Physicians Association

TABLE OF CONTENTS



ccpa news

SPECIAL EDITION 2021

Letter from CCPA/CCPAPP's Executive Director Kena Norris, MJ, FACHE

Despite what seems like a tiny speck of light at the end of the tunnel due to the COVID-19 vaccines, I am certain that we are all suffering from pandemic fatigue. And while the heartbreak remains for the countless lives who were lost, it seems that business as usual is slowly resuming in the United States. Thereby, it is a good time to reflect not only on how much the world has changed, but how we also changed as individuals.

Whether we were ready or not, the pandemic caused us to grow and adapt both personally and professionally. Collectively, we survived an era that started with pure panic, which was fueled by absolute uncertainty, to arrive where we are today. So instead of revisiting the 'pain points' caused by the pandemic, let's instead take the time to reflect on how medical professionals and their practices grew from it.

First and foremost, the pandemic showed us the resiliency of healthcare professionals as doctors, nurses, administrators, and staff had to learn entirely new skill sets. This resulted in a new competency in healthcare preparedness. And from this trial by fire, there were fundamental culture changes that will remain in medicine as we move beyond the pandemic. One of the most notable cultural shifts was the rapid adoption of telemedicine.

Thus, Children's Community Physicians Association has dedicated this special edition newsletter to the operational, legal and information technology issues posed by maintaining telemedicine visits in your practice. As we optimistically look towards a future, sans the daily challenges of COVID-19, we will collectively move forward with maintaining patient safety and access, and the continued viability of the medical practice.

Association Updates

Pediatric Telemedicine During Covid-19 and Beyond – Video Available

For CCPA members who were unable to attend the Pediatric Telemedicine During COVID-19 and Beyond event on June 16, 2021, the webinar is now available on the CCPA website at www.ccpaipa.org in the Members' Portal section. It is free of charge for members and can be watched at your convenience.

CCPA Member Benefits Reminder

Please be sure to check out the following new American Academy of Pediatrics' (AAP) new toolkits (Autism, ADHD and Mental Health) that are free to CCPA members and accessible on the AAP Pediatric Care Online™. The toolkits can be accessed via the CCPA website at www.ccpaipa.org in the Members' Portal section.

Also, as a reminder, CPR reimbursement is available up to $60 for all CCPA members. Please submit your paid invoice and a copy of your CPR card to ccpa@luriechildrens.org or by fax to 312.227.9526.

Lurie Children's Physician Services Webpage

The Physician Services' department has a new webpage, which can be accessed at luriechildrens.org/physicianservices. This site may be a useful resource to "favorite" or bookmark for future use because it includes:

- Satellite clinic schedules
- Quick reference guides
- Referral and consultation to/from Lurie Children's
- Contact resources at Lurie Children's
- Video library of virtual round table discussions on a variety of topics
- Community Provider Symposium Video Library
- LurieMD Provider Call Line (1.855.LurieMD or 1.855.587.4363)

CCPA News

CCPA News has expanded its content to cover pertinent healthcare law, practice management and other related issues using experts in these areas. If there is a legal, regulatory or practice management matter that you would like us to address in the newsletter, please contact LaVonna Swilley, CCPA Director of Operations at 312.227.7425 or lswilley@luriechildrens.org.

In the Spotlight

Did you know that CCPA has several members who are pediatric specialists? This section will provide a rotating spotlight on CCPA's subspecialists.

John T. B. Houston, MD

Children's Pediatric Urology Practice

childrenspediatricurology.com/

312.632.0032

Dr. John Houston has been on staff at Ann & Robert H. Lurie Children's Hospital of Chicago (formerly Children's Memorial Hospital) for over twenty years. Dr. Houston graduated from Yale University School of Medicine and he completed two years in general surgery and residency in urology at Baylor College of Medicine. Dr. Houston was the first African American fellow in the department of pediatric urology and in the Division of Surgery at Children's Memorial Hospital. In 2001, he became Chicago's first African American pediatric urologist and is currently one of two African American male pediatric urologists practicing in the United States today.

In addition, Dr. Houston is board certified in pediatric urology and specializes in treating patients with a range of pediatric urology conditions, including inguinal hernias, hypospadias, kidney reflux, urinary tract infections, incontinence, urinary obstruction, undescended testicles and other challenging situations.

Dr. Houston focuses on family and child wellness as it pertains to treating the pediatric urology health conditions. He and his staff look forward to the continuation of integrating this treatment method through in-person and telehealth visits. Dr. Houston has office locations in Chicago, New Lenox, Tinley Park and Westchester.

The Health of Telehealth Security: Tips to Protect Your Patients and Your Practice

By Brett Danis, SummIT Tech Partners, Inc.

As physicians and practices prepare for what life looks like in a post-pandemic world, one of the many concerns they will have to address is Information Technology (IT) security while providing healthcare virtually.

Telemedicine visits and working remotely, for better or worse, are here to stay.   However, the sheer speed of this pivot to telehealth is a cause for concern as it pertains to IT security – and providers need to have appropriate guardrails in place.

The numbers revealed by a new Bitglass study are alarming — there was an increase in healthcare cyber-attacks of over 55% in 2020, with an estimated impact to protected health information (PHI) of nearly 26 million people. The total count of healthcare breaches in the United States rose from 386 in 2019 to 599 in 2020 and IT related incidents accounted for nearly 70% of those breaches.

> There was an increase in healthcare cyber-attacks of over 55% in 2020.

This increase can be attributed in part to opportunistic hackers who see telemedicine as low hanging fruit. The unexpected rapid shift in the healthcare ecosystem last year created an environment ripe for nefarious actors to attack, as vulnerabilities were - and still are - often overlooked.

In 2020, we were forced to adapt to extraordinary circumstances, and now in 2021, we are in a year of rebuilding. It is time to pause and focus on what you can do to provide a safer virtual experience for you and your patients.

Your electronic medical records partner or telemedicine provider will have the foundational securities in place. However, that's not enough. Additional defenses for your practice to consider include:

- **Antivirus and Anti-Malware**: This is not optional. Your laptops, workstations, and servers should have comprehensive protection that is active, up-to-date and also scan devices on schedule. This goes double for 'work-from-home,' family shared devices. Enterprise antivirus software products are the best way to safeguard you against computer viruses and various malware such as ransomware, Trojan horses, spyware, adware, identity theft and more.

- **E-mail Protection**: E-mail has become a primary communication channel and sharing PHI through this avenue is now common, if not expected. These transactions through e-mail must be encrypted, protecting all parties. Secure, Health Insurance Portability and Accountability Act (HIPAA) compliant e-mail should utilize the Advanced Encryption Standard (AES), which encrypts both messages and attachments in transit and in storage. Your e-mail provider should also have a signed business associate agreement (BAA); a written arrangement that specifies each parties' responsibilities when it comes to electronic protected health information (ePHI) transmission.

- **Data Back-Up**: Ransomware is making headlines now more than ever and it is a threat that can shut a practice down. You should consider cloud-based offsite backup options that are HIPAA compliant and encrypted. Backing up your practice's data also protects your records from hard drive failure, data corruption and theft. It is an insurance policy that you do not know you need until it's needed, but you will be glad that you have it. Work-from-home models are the new normal, which means risks for ransomware related incidents are far and wide.

- **Virtual Health Platform**: Popular platforms like Apple FaceTime, Zoom, Microsoft Teams and Skype for telemedicine purposes were (and are) widely utilized to facilitate virtual health visits. However, if you recall some of the 'Zoom bombing' incidents last year, the rapid adoption of these apps for virtual visits created cybersecurity risks. Some virtual platforms have updated their security, however, if your organization has embraced telehealth, transitioning to an enterprise, health-care specific product would be prudent.

- **Staff Attention and Accountability**: In our opinion, human behavior is the number one vulnerability in cybersecurity. It is critical that you and your staff are aware of the risks and are taking the necessary precautions to keep your patients' information safe. Typically, user interaction has been ground zero for virus infections, ransomware attacks, and data breaches. By taking a people-centric approach to cybersecurity, putting policies in place, and educating your staff, you can deploy a strong last line of defense. Thus, protecting your practice and patients against the ever-evolving landscape of cyber security threats.

Brett Danis is the owner of SummIT Tech Partners, Inc. and is available to answer any questions you may have. SummIT's team of engineers are also available for risk analysis consultations. Simply e-mail them at support@summ-IT.com or call 773.717.0879. ●

Telemedicine: Here to Stay!

By Richard H. Tuck, MD, FAAP

Telemedicine has been around for years, but with limited application. It was primarily provided by on-demand commercial enterprises such as Teledoc as pediatric practices were slow adopters. However, this changed dramatically with the arrival of COVID-19, and its required social distancing demand. As pediatric practices suffered from the drastic decline in face-to-face patient visits, telemedicine access and visits sky-rocketed to provide patient care. Although telehealth use has fallen from its peak in April 2020, it remains a significant aspect of current health care delivery. This article will trace the history, the evolution, and the detailed business application of telemedicine in the medical home. Although the specifics of its future are uncertain, it is here to stay.

What, Where and How?

Telemedicine is virtual care and provides a real-time connection between patients and providers, as well as professional to professional. This digital service provides high value benefits but is associated with risks and challenges. Randomized trial results support telemedicine to be of equal quality for some conditions yet limited by the inability to complete a full examination and provide ancillary testing. Telemedicine is particularly helpful for less acute problems and for addressing mental health issues. Virtual care should achieve safety and effectiveness, improve efficiency, control costs, and respect patient values and perspectives.

How to Incorporate in Your Practice:

Telehealth visits can be provided from multiple locations for patient and provider. It does require a quiet well-lit space. However, some payors will not allow telehealth visits from any location other than the provider's practice. A quality telehealth vendor should be Health Insurance Portability and Accountability Act (HIPAA) compliant and ensure the privacy of patient information. They should offer appropriate technology for your practice, an easy user interface for providers and patients. Some telemedicine vendors will integrate into your electronic health record (EHR) system, or you may have an EHR with integrated telehealth capabilities, including scheduling and broadcast messaging.

> The AAP offers a telemedicine toolkit for digital health implementation

Additional considerations include enhancing your nonverbal communication "webside" manners, such as sitting up and leaning forward attentively with eye contact and heightened facial expressions. Clinicians should pay particular attention to their patient's reactions and speech patterns.

Annual preventive medicine visits are particularly challenging without an appropriate physical examination and opportunity to provide screenings, lab work and scheduled immunizations. Therefore, thoughtful incorporation of some aspects of the physical examination with virtual modalities is also a consideration, recognizing that the inability to "lay hands on" patients can be limiting. Establish standardized quality protocols, while understanding each digital experience should be personalized to fit the need of the patient and their family. Finally, recognizing that some in-person components will need to be provided at a future visit.

Moreover, practices should consider the promotion of your telehealth services to your patients. A printout explaining your virtual services, how to access and basic information related to charges is helpful. Also, promote these services on social media and your website. Educate your staff on access to these services, especially your front office staff.

As you consider how to incorporate telemedicine in your practice, turn to the American Academy of Pediatrics (AAP) resources for a step-by-step process. The AAP offers a telemedicine toolkit for digital health implementation. If you currently offer telemedicine services, this will assist with improving the telemedicine experience for you and your patients and families. It includes HIPAA and security requirements, vendor considerations, training resources, staffing, scheduling, and workflow issues. It will enable you to identify as well as work on your current areas of weakness. Allowing you to maximize payment, minimize work/hassle, and minimize liability related to these here-to-stay telehealth services.

The American Medical Association (AMA) has also recently launched a Telehealth Immersion Program. This is aimed at helping providers optimize and expand telehealth programs, and setting up a stabile long-term strategy.

Coding for Telehealth Visits:

As with all the services you provide, you must be current with ICD-10-CM (International Classification of Diseases, Tenth Revision, Clinical Modification) and Current Procedural Terminology (CPT) coding guidelines. The extensive list of CPT codes that may be used for synchronous interactive audio and video telemedicine services is provided in Appendix P in the CPT book. They are, with some exceptions, many of the same E/M (evaluation and management) codes for in-person encounters. Modifier-95 is appropriately used with these CPT codes, indicating they are delivered using a real time audiovisual encounter.

The other important required documentation is the place-of-service for telehealth outpatient office service: POS2 (place of service 02). Having provided these coding recommendations, different payors have requirements which may vary from these standard coding guidelines. Check with your individual payors for their requirements.

Documentation Requirements:

Knowing the documentation requirements and integrating them with your EHR is critical for telemedicine as it relates to payment during and post the pandemic. The required documentation is similar to face-to-face visits. And it should include the method of telecommunication, carefully documented time, and other elements of medical decision-making supporting E/M code selection. This needs to be supported with a separate, permanently retained written or recorded communication of the interactive two-way telecommunication. This must be HIPAA compliant, although with COVID-19 driving telehealth forward, special exceptions have been made during the declared current health care emergency, temporarily allowing for non-HIPPA compliant tools, including Facetime and Zoom.

Payment for Telehealth Visits:

It is critical that your practice be compensated appropriately for virtual services. The surge in telemedicine was facilitated in part by changes in government policy, which temporarily expanded what telemedicine services could be reimbursed. Prior to the pandemic, telemedicine was primarily used in rural and remote locations to improve access via videoconference visits with specialists. With the COVID-19 pandemic, Medicare has set the bar by expanding telephone and videoconference visits for all Medicare patients in their homes. This change was then widely adopted by other managed care payors in the United States.

Unfortunately, some clinicians have abandoned telemedicine, partially related to uncertainty about telemedicine's financial sustainability. There is also payor concern that due to the ease and improved access to care via telemedicine, there will be medically unnecessary care provided and fraudulent ordering of diagnostic tests. With the tremendous increase in these telehealth services and billing, Medicare predictably is pursuing fraudulent billing, a real and growing concern.

Furthermore, payment for telemedicine visits is a significant area of debate. Currently, payment is generally equivalent to face-to-face E/M visits. The AMA's telemedicine guides provide up-to-date coding and billing policies for audio as well as video calls. Some practices are billing for phone calls and portal messages, too. Ongoing conversations with your key payors related to the above payment issues are important.

The Future of Telehealth:

Realistically, there is no going back. Medicare, Medicaid, and other payors recognize the need to continue access to care via these high value services. State legislatures everywhere are acting to support the recognition of and payment for telemedicine. Federal legislation is being promoted with bills within the House and Senate aimed at expanding telehealth access, which are currently focused on Medicare, Medicaid, and CHIP beneficiaries.

Despite this, some payors are planning to cut back on access to telehealth services. Time will tell how this is received by all constituents. Millennial patients are demanding the convenience and rapid access provided by virtual services. It is also important to address healthcare equity as telemedicine is considered now, and in the future, i.e., does the patient and family have access to the technology and an internet connection necessary to make telemedicine visits a practical reality?

Finally, the question remains, will telemedicine become a standard of health care for your practice in the future? If so, consider incorporating specific questions related to telehealth in your practice evaluations and patient surveys. It is important to maintain positive provider and patient experiences whether in-person or virtually. ●

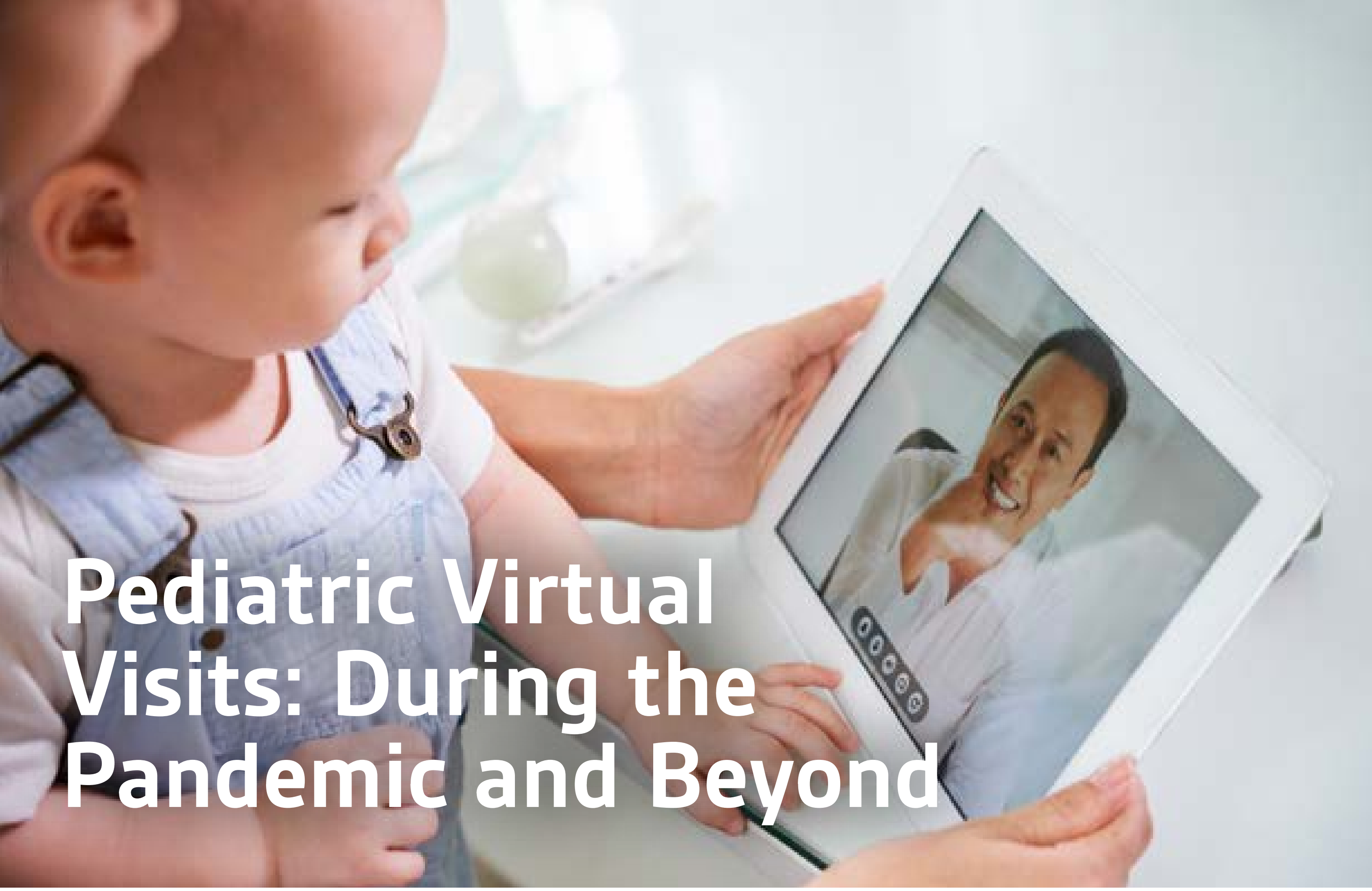
Resources:

American Academy of Pediatrics

- Practice Resource Center: www.aap.org
- The AAP Parenting Website: www.healthychildren.org

American Medical Association

- AMA Telehealth Immersion Program: www.ama-assn.org



Pediatric Virtual Visits: During the Pandemic and Beyond

By Michael J. Sacopulos, Founder and CEO, Medical Risk Institute

In early 2020, we saw the dawn of a pandemic that we were all unfamiliar with and the medical community responded with amazing speed and courage. For once, regulators stepped out of the way and let physicians practice with waived patient privacy and reimbursement regulations. Allowing telemedicine to move center stage. The broad-based success of telemedicine during 2020 marks a vast change in the practice of medicine. Telemedicine has come of age. This article will help providers to identify and address issues to establish a safe, compliant telemedicine practice.

Before jumping into the telemedicine weeds, we should first acknowledge telemedicine's popularity. The vast majority of patients and providers like telemedicine. A J.D. Power telehealth satisfaction study in 2020 found, "The overall customer satisfaction score for telehealth services to be 860 (on a 1,000-point scale) which is among the highest of all healthcare, insurance, and financial services industries studied." Another study from the American Medical Association (AMA) found 80% of patients reacted favorably to the use of telemedicine. However, it was not just patients that reacted positively, 68% of providers reported to the AMA that they were motivated to increase telehealth in their practices. The strength of these statics should make the remaining providers consider converting to telemedicine.

One of the best sources for a compliance overview for telemedicine comes from the Federation of State Medical Boards (FSMB). "The Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine" from the FSMB identifies many of the issues that need to be met when establishing a compliant telemedicine practice.

Licensing is one of the first requirements addressed by the FSMB policy. Physicians must be licensed in the state where the patient is located. This means a physician practicing telemedicine may need to be licensed in multiple states if their patient population crosses state lines. As an example, Chicago based physicians who see children from northwest Indiana, will need an Indiana license. Many may feel this is an impediment to practicing telemedicine, but the Interstate Medical Licensing Compact (IMLC) is designed to assist physicians in securing licenses in multiple states. The general idea is that a physician has a state of principal licensure. The physician then prepares an application to receive documents from his or her principal licensure called "Letters of Qualification." These Letters of Qualifications are then transferred to the state where the physician is not licensed, to receive an expedited license to practice medicine. Becoming licensed in any state is never a hassle-free experience, however, the IMLC greatly reduces the transactional friction associated with acquiring a new license.

Another issue when practicing telemedicine is determining which patients can be seen remotely, which will require a state by state analysis because "when" telemedicine can be used varies from state to state. Some states require the patient to be seen in person before qualifying for future telemedicine visits. Other states allow a provider to see new patients via telemedicine. As you already know, the global pandemic opened the door for telemedicine regardless of state regulations. Some states suspended these rules and have unclear laws relating to telemedicine and establishing patients, which has currently left this area of law in flux. Illinois law does not speak to the establishment of the physician/patient relationship via telemedicine. The establishment of a physician/patient relationship in Illinois is deferred to the medical judgment of the treating physician.

Like all medical encounters, informed consent from the patient is necessary for treatment. Informed consent in the telehealth world comes with unique requirements.

The FSMB tells us that informed consent in telemedicine begins with the identification of the patient, the physician, and a description of the physician's credentials. The patient should have a clear understanding of the types of transactions that are permitted using telemedicine technologies, and the patient must agree that the physician determines whether or not the condition being diagnosed and/or treated is appropriate for a telemedicine encounter. The patient also needs to understand the security measures being employed for telemedicine such as data encryption, multifactor identification, etc. Informed consent documents should include a hold harmless clause for information that may be lost due to technical failures during the patient encounter. Finally, the patient should expressly consent to allow their patient identifiable information be forwarded to a third-party if necessary. A standard informed consent for telemedicine visit should be created by any clinician seeing patients remotely.

A requirement found in the FSMB's model policy which often surprises physicians involves the emergency service referrals. There needs to be a written protocol of where patients may seek emergency services. This is not a problem if the patient is in the same geographic area of the provider. But whenever patients are outside of their area, physicians need to be prepared if an emergency is identified during a telemedicine encounter.

Next, we should consider medical documentation. Charting for a virtual visit should be the same as if the patient were in your exam room. Medical documentation should confirm that the telemedicine informed consent process was properly completed. Medical records from telemedicine visits are subject to the same rules and regulations as in-person encounters, including the open note requirements and information blocking rules found in the CURES Act. Providers should also be aware of a recent "right of access" initiative by the Office of Civil Rights (OCR), which is aimed to address patients being able to access their medical records in a timely and cost-effective fashion.

> The Illinois Telehealth Act does not provide any regulation on issuing online prescription for telemedicine. Whether or not a provider should prescribe medication online to his or her patient is up to the provider's professional judgment in Illinois.

Perhaps one of the primary concerns for telemedicine relates to patient privacy. Telemedicine visits must take place on a secure platform. There are several platforms which are compliant with the Health Information Technology for Economic and Clinical Health Act (HITECH) requirements when communicating with patients. Examples of some appropriate and compliant platforms include Zoom for Healthcare, Doxy.me, Tiger Connect and Amazon Chime. Unfortunately, during the pandemic we have seen patient encounters that were hacked on less secure platforms.

Another area of concern is prescribing. Traditionally, whether medication could be prescribed via a telemedicine encounter was controlled on a state by state basis. Some states forbid the issuing of a prescription to a patient that has not had an in-person visit. Other states are less restrictive. For example, the Illinois Telehealth Act does not provide any regulation on issuing online prescription for telemedicine. Whether or not a provider should prescribe medication online to his or her patient is up to the provider's professional judgment in Illinois. As previously mentioned, the rules that apply for telemedicine is the state where the patient is located. Just because the provider is located in Illinois does not mean they are exempt from other state's laws and regulations which the patient is located.

Providers also need to be appropriately insured before conducting telemedicine appointments. Insurance for this activity falls into two broad categories. First, there is professional liability or traditional medical malpractice and defense coverage. Remember you are practicing in the state where your patient is located,

therefore you should know what coverage is required in those states. Consult with your insurance broker to guarantee that you have appropriate professional liability for each state in which you will be practicing in remotely. The second broad category is cyber insurance. Recent months have seen an uptick in ransomware and cybercrime against medical providers. Whether practicing telemedicine or not, medical practices need cyber coverage. The need for cyber coverage is simply made more acute for remote patient encounters. Again, work with your insurance broker to acquire appropriate cyber insurance for your practice.

Moreover, there are some ethical issues that present themselves whenever treating patients remotely. When a child presents in your exam room, the child's home environment is not always clear. Telemedicine can take us into the patient's home. Imagine a telemedicine encounter where your patient is sitting at the kitchen table, but there's also a 9mm pistol on that same table. This and other unsafe home conditions can be detected during a telemedicine encounter with a child. Pediatricians need to be prepared to address these situations. A detailed description of ethical concerns arising from telemedicine encounters is beyond the scope of this article. However, it is appropriate when moving into this area of practice to think about these issues.

Finally, telemedicine post pandemic will likely see an expansion with rule and regulations alterations. As such, providers need to remain on top of these changes. There are several great resources for telemedicine updates such as the American Telemedicine Association. Centers for Medicare & Medicaid Services (CMS) also provides good guidance as does the Federation of State Medical Boards. Finally, you may want to be on the OCR email list. OCR sends out useful emails regarding telemedicine issues. While all of this may seem daunting, establishing your practice's telemedicine infrastructure will take just a little time. However, once the initial work is completed, telemedicine visits can be a satisfying alternative for patients and providers. ●

The views and opinions expressed in CCPA News are those of the authors and do not necessarily reflect the views of CCPA.