June 1, 2020: Developing a Telemedicine Program – Technology
Questions submitted during Mike Holcomb's presentation:

- **How can we use multiple forms of video, music and demonstration in a platform?**
  Different platforms have different capabilities, but many have audio and video playback capability along with the ability to show views from peripheral cameras. Can you provide more detail on the use case your are working on? There is a relatively new Digital Health Directory that includes some telehealth platform vendors: https://www.techhealthdirectory.com/ that may be of interest.

- **With MIPS/Medicaid Billing, we have to have a HIPAA, FERPA, and IDEA compliant site. Providing OT, is Zoom the only platform that allows this while giving tools like whiteboards that can be shared between the student and the provider?**
  No, there are many platforms that are HIPAA compliant and offer tools like whiteboards and content sharing. There is a relatively new Digital Health Directory that includes some telehealth platform vendors: https://www.techhealthdirectory.com/

- **Which platform do you recommend? Zoom or Skype?**
  We don't recommend a specific platform. We do recommend using a platform that is intended for healthcare use. If the platform is hosted/managed by a 3rd party service/contractor, versus by the healthcare provider internally, then a business associate agreement (BAA) is a legal requirement. If the 3rd party provider/contractor will not sign a BAA in association with their services handling protected health information then we recommend looking for a 3rd party provider that will sign a BAA. There is a relatively new Digital Health Directory that includes some telehealth platform vendors: https://www.techhealthdirectory.com/

- **Is there a way to prevent the patient from screen recording the session?**
  Generally, I would say no except if you provided hardware and software to the patient that was locked down preventing them from modifying the hardware and software. The patient, however, could still surreptitiously record the session using an external video recorder. I suggest consulting your legal counsel about including a provision in your terms of service in which the patient agrees to that requires them to agree to not record the session unless specifically authorized by the provider to do so.

- **Are there specific internet capabilities internet providers should have embedded to support secure connections? Clearing cookies?**
  Internet providers may provide a security software such as antivirus that subscribers can run on their computers, and often have firewall capabilities built-in to the routers that are used to connect the subscriber to the Internet service, but don't typically take responsibility for clearing cache or cookies on a subscribers own equipment such as computers or mobile devices. Please see this AMA document https://www.ama-assn.org/system/files/2020-04/cybersecurity-work-from-home-covid-19.pdf regarding computer and device security measures and let me know if you have any additional questions or need additional information.

- **Is there a concern for having providers use personal devices to provide telemed services if the API is secure?**
  Each organization should have a policy regarding the use of personal devices that takes into account the risks of personal device use and prescribes when a personal device may be used, including a list of approved devices, and for what purposes those may be used and in what contexts. Generally speaking all devices and software applications that they run have some vulnerabilities. Devices that are centrally managed by the organization can, if managed pro-actively with security updates and application patching, generally provide a much more secure endpoint for providers to use to conduct telehealth visits.

- **In a country where HIPPA compliance is not mandatory, should we still strive to get tech services that are HIPPA?**
  HIPAA is good business practice in that its goal is to keep patient information accessible to only those that need it for the provision of patient care, and to the patient and to people that the patient designates as authorized to have access. In a country that doesn't require HIPAA, it is likely the there are some other laws regarding patient privacy that need to be observed by healthcare providers. Please seek legal counsel in your country for specific advice on laws that your healthcare provider organization needs to comply with.

- **How to prevent your session from being hacked?**
  Use a platform intended for healthcare use, with a business associate agreement (required when 3rd party provider has access to protected health information) if needed, that incorporates security measures such as password protection for sessions, encrypted communications, virtual waiting rooms (people connect to the waiting room and then are admitted to the session by the provider/host vs joining the session directly). In addition use devices that are not end-of-life (meaning no longer receiving security and other patches), that are fully patched with all available security updates, are not running untrusted applications, are running antivirus/antimalware software, are maintained and monitored by qualified IT personnel etc.

- **In types of assessments is it possible to gather data such as analyzing movement quality of movement or videos of movement?**
  I don't understand the question in relation to securing telemedicine communications. Please feel free to contact me to discuss.

- **I work as a telehealth facilitator w/in an assisted living facility. The facility has a good firewall, but should I have an extra layer of security?**
  Yes, workstations / devices and software should be kept up to date with all the latest security patches and should run anti-virus/antimalware software to prevent malicious code from infecting them such as if someone accidentally clicks on a phishing email link. Utilize platforms that are intended for healthcare use and that incorporate security features that you can utilize to secure your communications.

- **What is the best practice in acquiring remote signatures on documents and having them return to the EHR database?**
  This could be accomplished by working with the EHR vendor to either have them add this capability directly to their EHR implementation or to work with the EHR vendor and a 3rd party e-signature service to develop a workflow that utilizes the 3rd party e-signature

service and routes signed documents back to the appropriate record in the EHR, with appropriate business associate agreements in place.

- **Saving recorded visit within the EMR**
  You'll need an EMR that facilities this storage capability. If this is not handled directly within the EHR, you would need to work with the EHR vendor and any 3rd parties involve in recording and storing the video of the visit to develop a workflow to capture the recording of the visit and then link or transfer the video to the EHR properly associated with the correct patient record. All of this incorporating any required business associate agreements and security measures to make sure that only authorized individuals can access the recordings and that they remain secure over time.

- **What if patient has others in the home, such as children**
  The healthcare provider should work with the patient to try to find an environment appropriate for the telehealth visit, or at least provide some suggestions about how to handle this situation. How would the patient handle the care of others if they were seeing the healthcare provider in person? Please see item 7 at this website: https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

- **What is our responsibility when patients do not place themselves in a secure/private area?**
  The healthcare provider should work with the patient to try to find an environment appropriate for the telehealth visit, or at least provide some suggestions about how to handle this situation. Can the patient use a headset and lower their voice, or move to a more private area? Please see item 7 at this website: https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

- **When is a HIPAA business associate agreement required and what is it?**
  Business associate agreements (BAA) https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html are a primary key to HIPAA compliance when hiring a 3rd party service that will be permitted to access a patient's protected health information (PHI) https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected
  If the 3rd party is not willing to sign a BAA https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html then look for another 3rd party provider that will. A BAA agreement is legally required if a healthcare provider (covered entity) allows a 3rd party business access to electronic protected health information about the health providers patients. Other important aspects to consider in terms of HIPAA compliance include the technical, administrative and physical safeguards utilized to protect and secure any patient protected health information that the 3rd party has access to.

- **What part of the environment has to be compliant?**
  (https://hipaaqsportal.hhs.gov/a/dtd/What-part-of-the-environment-has-to-be-compliant/122279-36899)

- **Does the entire environment need to be HIPAA compliant, or is it possible that the solution could fall into an exception to HIPAA, or can they use an API to store certain kinds of data? If you're building modern technologies, you're relying on a lot of third party (likely API) based services; mostly cloud based services. So which aspects of those need to be compliant?**
  Both business associates and covered entities must consider where and how they use, maintain and disclose protected health information in order to determine how to comply with the HIPAA Rules.
  The business associate is responsible for ensuring its compliance with the applicable HIPAA standards for all aspects of the environment that involve PHI and the provision of business associate services or activities.

  Your organization's legal counsel, HIPAA Privacy Officer, and Information Security Officer should ultimately provide a determination on whether or not a particular service can be used with regard to complying with HIPAA and other privacy and security laws.

Michael Holcomb
Associate Director, Information Technology
Arizona Telemedicine Program http://telemedicine.arizona.edu
University of Arizona
520-626-4496
mholcomb@telemedicine.arizona.edu

Search for Telemedicine and Telehealth Clinical Providers using the:
National Service Provider Directory