Managing Clinical Risks Associated with Telehealth Programs

The Health Resources and Services Administration (HRSA) defines telehealth as the use of electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education, public health, and health administration.

Telehealth uses different technologies to deliver care, including the following:

- Live videoconferencing, which allows two-way audio and visual information to be transmitted between the patient and physician, or between providers, in real time. This is also known as synchronous telehealth.
- "Store and forward," in which patient information, such as an image or data, "stored" in the originating facility's computer system is securely "forwarded" to the telehealth provider at the distant site for review. Store and forward allows information to be interpreted at a later time.
- Remote patient monitoring, in which vital sign information (e.g., blood pressure) and other data (e.g., blood glucose levels, indicators of fetal well-being) are collected by monitoring devices, usually at home, and transferred to the patient's physician. This technology is used often in the care of patients with chronic conditions.
- Mobile health (mHealth), in which healthcare and public health information are communicated through mobile devices. The information may include general educational information, targeted texts, and notifications about disease outbreaks.

Telehealth has the potential to greatly improve access to and use of healthcare, particularly for rural or underserved areas. In 2018, 43% of all health centers reported using telehealth to provide remote clinical care services. With HRSA providing additional resources and funding opportunities, health centers are increasingly using telehealth as a means of delivering primary care, chronic condition management, specialty care, mental health services, and oral health services to patients.

As the expansion of telehealth continues, robust clinical, operational, and technical telehealth processes are necessary in order to increase patient safety and limit risk. Health centers and free clinics can use the following checklist to prevent, identify, and manage clinical risks associated with developing, implementing, and maintaining a telehealth program.

1. Telehealth Program Development

☐ A. Create a multidisciplinary team to evaluate the feasibility of implementing a telehealth program. Include providers and representatives from senior leadership, information technology, risk management, finance, human resources, and quality improvement.

☐ B. Collaborate with your regional telehealth resource center for assistance, education, and information about providing telehealth services, including resources for telehealth program development.

☐ C. Evaluate telehealth needs of your specific patient populations and define the telehealth services your program will deliver based on those needs.

☐ D. Assess your health center's readiness for telehealth and create an action plan to address any identified gaps.

☐ E. Incorporate appropriate evaluation measures to assess the quality of your telehealth program and identify potential opportunities for improvement. Include patient and provider satisfaction measures.

☐ F. Monitor national policy and current state laws related to telehealth and determine whether any changes affect the organization's telehealth program. Extraordinary circumstances may accelerate changes in policy. For example, the COVID-19 pandemic led to interim telehealth policy changes at both the federal and state level in order to facilitate the rapid adoption of telehealth services across the country.

Notes:

2. Privacy, Security, and Patient Confidentiality

☐ A. Verify with the software manufacturers that all telehealth technology complies with the Health Insurance Portability and Accountability Act (HIPPA) security rules for protecting electronic protected health information (ePHI). The technology should include features such as fully encrypted data transmission, user authentication, and secure connections. A security risk assessment tool or a telehealth security self-assessment questionnaire (see Table 3) may enhance verification, which should take place before the organization enters into a business associate agreement (BAA). Certain common videoconferencing platforms (e.g., FaceTime, Skype) and even standard text messaging do not fulfill HIPAA requirements.

- In response to the COVID-19 nationwide public health emergency, the Office for Civil Rights, a division of the U.S. Department of Health and Human Services, issued a notice indicating that it will not impose penalties against covered healthcare providers for the lack of a BAA with video communication vendors or for any other noncompliance with the HIPAA rules related to the good faith provision of telehealth services during this emergency. Consider additional

guidance in using nontraditional telehealth technology during the public health emergency.

☐ B. Ensure only authorized users have access to ePHI.

☐ C. Monitor secure communication systems to prevent accidental or malicious breaches.

☐ D. Hold telehealth appointments in a private location where visits cannot be overheard.

Notes:

3. Patient Education and Informed Consent

☐ A. Educate patients about telehealth, including its risks and benefits, alternatives if available, and the limitations of the equipment and technology. Use teach-back methods to ensure the patient's understanding of telehealth services.

☐ B. Walk patients through a virtual visit, and consider doing a trial run while the patient is at the health center. Staff should have access to customized scripts designed to cover detailed aspects of the telehealth visit, including the purpose of the visit, how long the visit will take, and what to do if there is a technology failure. Scripting should also include step-by-step directions to instruct patients on launching the visit from compatible home equipment (if applicable) and interacting with their telehealth provider.

☐ C. Provide patients with a written telehealth preparation checklist (see p. 118) that includes equipment specifications and what to expect during the visit.

☐ D. Review your state's requirements for telehealth consent (select your state on the map, then scroll to "Consent") and incorporate requirements into your telehealth program. Some states may require consent each time telehealth is used. Even if your state does not require telehealth consent, it is best practice to obtain the patient's informed consent.

☐ E. Obtain the patient's written informed consent (see this example live form as well as AHRQ's easy-to-understand telehealth consent form for guidance), documenting education provided to the patient about telehealth and his or her understanding, before providing telehealth services to the patient.

- Collaborate with local legal counsel to ensure that patient electronic signatures for telehealth consent meet state and local requirements. Although electronic signatures are not specifically addressed by HIPAA, the Electronic Signatures in Global and National Commerce Act establishes criteria for electronic signature validity at a national level. Most states have also adopted the Uniform Electronic Transactions Act or similar state laws. Criteria for valid electronic signatures often include a clear intent to sign and consent to do business electronically; a

record of signature with information on how the signature was captured; and a way to access the signed documents for later reference (such as a function for patients to print after signature or an option to receive a copy by mail).

Notes:

4. Credentialing and Privileging

☐ A. Verify that remote practitioners are qualified to practice telehealth medicine in the areas in which they are requesting telehealth privileges. Particular consideration should be given to situations where telehealth services cross state lines. Check whether your state belongs to the Interstate Medical Licensure Compact, which may offer a streamlined process to obtain licensure to practice in multiple states.

- Please note that many states are currently taking actions to remove barriers to provide telehealth during the COVID-19 public health emergency, including temporarily waiving licensure requirements.

☐ B. Keep track of state laws that may affect the practice of telehealth and consult with local legal counsel to ensure legal telehealth requirements are met.

☐ C. Incorporate selected clinical telehealth performance measures into your health center's privileging processes. Monitor for adverse outcomes and discrepancies in diagnosis, treatment, and follow-up between telehealth and face-to-face visits.

Notes:

5. Equipment and Technology

☐ A. Determine your health center’s equipment needs in collaboration with your vendor and conduct a comprehensive technology assessment prior to purchasing any new equipment. Be sure to include hands-on testing of the equipment with the providers and staff who will be using the equipment.

☐ B. Verify that all telehealth hardware and software is compatible with your electronic health record (EHR).

☐ C. Conduct routine equipment testing and maintenance to address potential problems before they affect patient care. Include ongoing quality checks of audio, video, and data transmission functions.

☐ D. Perform equipment calibration before every telehealth visit and document results.

☐ E. Ensure that future technology upgrade costs, including equipment and associated software, are accounted for in your telehealth business plan.

Notes:

6. Provider and Staff Education

☐ A. Train providers and staff on telehealth topics, including the goal of the telehealth program, key roles and responsibilities (see p. 115), policies and procedures, and quality metrics.

☐ B. Identify telehealth "superusers" within the health center who can assist other users with telehealth processes and help communicate when processes change.

☐ C. Develop instructions for staff on what to do in the event of equipment malfunction.

☐ D. Train staff regularly on the various ways an organization may be hacked by cybercriminals, and on how to prevent security breaches.

Notes:

7. Conducting Telehealth Visits

☐ A. Recognize that practicing medicine via telehealth requires meeting the same standard of care as face-to-face encounters. During the visit, if it is determined that telehealth is not appropriate for the patient's individual situation and medical needs, the provider should arrange for alternative evaluation and treatment.

☐ B. Ensure that a lawful patient-provider relationship exists or can be properly established during the telehealth visit according to state laws. In some cases, when the patient is new the telehealth provider may have to conduct a face-to-face exam before telehealth can be used or consult another provider who already has an established relationship with the patient.

- Please note that many states are currently taking actions to remove barriers to provide telehealth during the COVID-19 public health emergency, including temporarily streamlining requirements for establishing a patient-provider relationship.

☐ C. Use a preparation telehealth etiquette checklist (see p. 114) to ensure that professional standards are upheld during the visit. Preparation checklists focusing on specific clinical telehealth topics should also be developed and made available to providers and staff assisting with the telehealth visit.

- For example, telehealth providers in the primary care setting can use this guide on conducting remote consultations for COVID-19, which is based on data made available in March 2020 in response to the national public health emergency.

☐ D. Follow federal and state laws regarding online prescribing. The Ryan Haight Online Pharmacy Consumer Protection Act of 2008 imposed a federal prohibition on form-only online prescribing for controlled substances, with some exceptions:

- Certain providers may be exempt from the act when using telehealth to provide medication-assisted treatment.

- On March 16, 2020, the Drug Enforcement Administration (DEA) published a COVID-19 information page to provide guidance relating to the COVID-19 public health emergency, including the ability to prescribe controlled substances via telehealth without a prior in-person exam.

☐ E. Document any provider-patient interactions using telehealth services in the EHR. Telehealth visit documentation should contain the same elements as records for a face-to-face encounter (e.g., reason for visit, history, review of systems, medical decision-making, and treatment plan). Include a statement indicating that the visit was provided via telehealth, noting the location of the patient and the names and roles of any other providers or staff participating in the visit.

Notes:

Want to learn more? Refer to the guidance articles The HIPAA Security Rule and The HIPAA Privacy Rule, the Get Safe! High Efficiency or High Risk? Using Technology to Communicate with Patients, and the Credentialing and Privileging Toolkit. Additional information is also available on HRSA's Bureau of Primary Health Care homepage, PAL 2020-01 Telehealth and Health Center Scope of Project, and Health Center Program COVID-19 Frequently Asked Questions (FAQs).

Clinical Risk Management Program resources are provided for FREE by ECRI on behalf of HRSA. Don't have access or want to attend a free, live demonstration of the website? Email Clinical_RM_Program@ecri.org or call (610) 825-6000 ext. 5200.

Information provided by ECRI is intended as guidance to be used consistent with the internal needs of your organization. This information is not to be viewed as required by ECRI or the Health Resources and Services Administration.

This site is maintained by ECRI on behalf of the Health Resources and Services Administration. For questions regarding HRSA requirements, please refer directly to relevant HRSA policy and requirement documents.