AMERICAN TELEMEDICINE ASSOCIATION

CORE OPERATIONAL GUIDELINES FOR TELEHEALTH SERVICES INVOLVING PROVIDER-PATIENT INTERACTION

MAY 2014

Acknowledgements

The American Telemedicine Association (ATA) wishes to express sincere appreciation to the ATA Practice Guidelines Committee for their invaluable contributions in the research, writing and development of the following guidelines.

(Alphabetical Order)

ATA Standards and Guidelines Committee

Chair: **Elizabeth A. Krupinski, PhD,** Professor & Vice Chair of Research, Department of Medical Imaging, University of Arizona

Committee Members

Nina Antoniotti, RN, MBA, PhD, Director of Telehealth, Marshfield Clinic TeleHealth Network

David Brennan, MSBE, Director, Telehealth Initiatives, MedStar Health

Anne Burdick, MD, MPH, Associate Dean for Telemedicine and Clinical Outreach, Professor of Dermatology, Director, Leprosy Program, University of Miami Miller School of Medicine

Jerry Cavallerano, PhD, OD, Staff Optometrist, Assistant to the Director, Joslin Diabetes Center, Beetham Eye Institute

Helen K. Li, MD, Adjunct Associate Professor, University of Texas Health Science Center

Lou Theurer, Grant Administrator, Burn Telemedicine Program, University of Utah Health Sciences Center

Jill M. Winters, PhD, RN, President and Dean, Columbia College of Nursing

ATA Staff

Jordana Bernard, MBA, Senior Director Program Services

Jonathan D. Linkous, CEO

AMERICAN TELEMEDICINE ASSOCIATION

Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions

(An Update of the February 2008
"Core Standards for Telemedicine Operations")

Table of Contents

Preamble	**4**
Scope	**5**
Definitions	**5**
Administrative Guidelines	**6**
Clinical Guidelines	**8**
Technical Guidelines	**10**
Appendix: References	**14**

Preamble

The American Telemedicine Association (ATA) brings together diverse groups from traditional medicine, academia, technology and telecommunications companies, ehealth, allied professional and nursing associations, medical societies, government, military, regulatory and others to overcome barriers to the advancement of telemedicine through the professional, ethical and equitable improvement in health care delivery.

ATA has embarked on an effort to establish practice guidelines for telemedicine to advance the science, to assure uniform quality of service to patients, and to promote reasonable and informed patient and provider expectations. The guidelines are developed by panels that include experts from the field and other strategic stakeholders, and are designed to serve as both an operational reference and an educational tool to aid in providing appropriate care for patients. The guidelines generated by ATA undergo a thorough consensus and rigorous review including an open public commentary period, with final approval by the ATA Board of Directors. Existing products are reviewed and updated periodically.

The purpose of these guidelines is to assist practitioners in pursuing a sound course of action to provide effective and safe medical care that is founded on current information, available resources, and patient needs. The guidelines recognize that safe and effective practices require specific training, skills, and techniques, as described in each document. The resulting products are properties of the ATA and any reproduction or modification of the published guideline must receive prior approval by the ATA.

The practice of medicine is an integration of both the science and art of preventing, diagnosing, and treating diseases. Accordingly, it should be recognized that compliance with these guidelines alone will not guarantee accurate diagnoses or successful outcomes. If circumstances warrant, a practitioner may responsibly pursue an alternate course of action different from the established guidelines. A divergence from the guidelines may be indicated when, in the reasonable judgment of the practitioner, the condition of the patient, restrictions or limits on available resources, or advances in information or technology occur subsequent to publication of the guidelines. Nonetheless, a practitioner who uses an approach that is significantly different from these guidelines is strongly advised to provide documentation, in the patient record, that is adequate to explain the approach pursued.

Likewise, the technical and administrative guidelines in this document do not purport to establish binding legal standards for carrying out telemedicine interactions. Rather, they are the result of the accumulated knowledge and expertise of the ATA workgroups and other leading experts in the field, and they are intended to address the technical quality and reliability of telemedicine encounters. The technical aspects of and administrative procedures for specific telemedicine arrangements may vary depending on the individual circumstances, including location of the parties, resources, and nature of the interaction.

NOTE ON THIS UPDATE

This update has four key modifications: 1) enhances guidance on educating patients about telehealth treatment; 2) adds several new items related to verification of patient/provider identity and service delivery location; 3) provides guidance related to mobile devices and services delivered to patients in non-facility settings; and 4) expands guidelines on privacy and security requirements.

Scope

The following guidelines are fundamental requirements to be followed when providing medical and other healthcare services using telecommunications technologies, and any other electronic communications between patients, practitioners and other healthcare providers. The guidelines apply to individual practitioners, group and specialty practices, hospitals and health care systems, and other providers of health related services where there are telehealth interactions between patients and service providers for the purposes of health care delivery. These guidelines may apply to specialty services, but other guidelines and standards addressing specific specialties have been and continue to be developed by separate workgroups within the ATA and other professional societies. When guidelines, position statements, or standards from any professional organization or society exist, health professionals should also review these documents and, as appropriate, incorporate these into practice. These guidelines pertain primarily to healthcare professionals and patients located in the United States. In situations where either or both parties are not within the US, these guidelines may be referred to but any local guidelines that are in place **shall** be referred to and take precedence over these. [1,2]

Definitions

Terms and definitions that are commonly used in telehealth/telehealth are available on the ATA website. [3] For this document there are several terms that need to be defined specifically:

"*Telehealth*" - telehealth is the use of medical information exchanged from one site to another via electronic communications to improve a patient's health status. Telehealth includes a growing variety of applications and services using two-way video, email, smart phones, wireless tools and other forms of telecommunications technology. Telehealth is not a separate medical specialty. It is a delivery tool or system. Closely associated with telehealth is the term "telehealth," which may be used interchangeably with telehealth, but is sometimes used to encompass a broader definition of health care that uses telecommunications technologies. Videoconferencing, transmission of still images and other data, e-health including patient portals, m-health, remote monitoring, continuing medical education, and medical call centers, are all considered part of telehealth and telehealth (ATA, 2007).

"*Organization*" - includes organizations, institutions, and business entities, including online service entities.

"*Health professionals*" - refers to individuals.

"*Shall, should, and may*" - This document contains requirements, recommendations, or actions that are identified by text containing the keywords "shall," "should," or "may." "**Shall**" indicates a required action whenever feasible and practical under local conditions. These indications are found in bold throughout the document. "**Should**" indicates an optimal recommended action that is particularly suitable, without mentioning or excluding others. "**May**" indicates additional points that may be considered to further optimize the healthcare process. "**Shall not**" indicates that this action is strongly advised against.

Administrative Guidelines

Organizations

1. Organizations providing services via telehealth **shall** follow the standard operating policies and procedures of the governing institution. If the telehealth operation is a sole entity or part of a solo practice, that entity or solo practice **shall** have policies and procedures in place to govern all administrative functions that responsibly include and address aspects of telehealth with regards to:
   - Human resource management
   - Privacy and confidentiality
   - Federal, state, local, and other regulatory agency and ethical requirements
   - Fiscal management
   - Ownership of patient data and/or records
   - Documentation, including use of electronic health records
   - Patient and clinician rights and responsibilities
   - Network and data transmission, storage and access security
   - Use of equipment, devices and technology including peripheral devices, network hardware and associated software.
   - Research protocols (if applicable)
   - Technical and medical competence in the service provided, including training of all personnel involved in the telehealth operations (i.e., healthcare professionals, technical, administrative and other relevant staff)
   - Evaluation criteria
   - Availability of organization information (e.g., ownership, location, website, contact information)

2. Organizations providing telehealth should have in place a systematic quality improvement and performance management process that encompasses quality

assurance and quality control and complies with any and all organizational, regulatory, and accrediting requirements for outcomes management. This process should be reviewed and updated as appropriate on a regular basis.

3. Organizations and health professionals providing telehealth services **shall** ensure compliance with relevant local, state and federal (or international if appropriate) legislation, regulations, accreditation and ethical requirements for supporting patient/client decision-making and consent, including protection of patient health information. [4-9]

4. Organizations **shall** have a mechanism in place for ensuring that patients and health professionals are aware of their rights and responsibilities with respect to accessing and providing health care via telehealth technologies (whether within a healthcare institution or other environment such as the home, school or work), including the process for communicating complaints.

5. Organizations **shall** respect patients' requests for in-person care whenever feasible.

6. Prior to the start of the telemedicine encounter, the provider **shall** inform and educate the patient in real-time of all pertinent information such as: discussion of the structure and timing of services, record keeping, scheduling, privacy and security, potential risks, confidentiality, mandatory reporting, billing, and any information specific to the nature of videoconferencing. The information **shall** be provided in language that can be easily understood by the patient and/or caregiver, especially when discussing technical issues like encryption or the potential for technical failure. These topics may be provided orally or in writing.
7. Additionally, the provider or designee should set appropriate expectations in regard to the telemedicine encounter. This may include for example prescribing policies, scope of services, communication and follow-up. The information **shall** be provided in language that can be easily understood by the patient. This is particularly important when discussing technical issues like encryption or the potential for technical failure.
8. Key topics that **shall** be reviewed include: confidentiality and the limits to confidentiality in electronic communication; an agreed upon emergency plan, particularly for patients in settings without clinical staff immediately available; process by which patient information will be documented and stored; the potential for technical failure, procedures for coordination of care with other professionals; a protocol for contact between visits; and conditions under which telemedicine services may be terminated and a referral made to in-person care.
9. Organizations providing and/or receiving telehealth services that establish collaborative partnerships **shall** be aware of applicable legal and regulatory requirements for appropriate written agreements, memorandum of understanding, or contracts. Those contracts, agreements, etc., **shall** be based on the scope and application of the telehealth services offered, and **shall** address all applicable administrative, clinical and

technical requirements. All parties involved in such agreements should have an appropriate legal review conducted on the documents prior to signing.

Health Professionals

1. Professionals **shall** conduct care consistent with the jurisdictional regulatory, licensing, credentialing and privileging, malpractice and insurance laws and rules for their profession in both the jurisdiction (site) in which they are practicing as well as the jurisdiction (site) where the patient is receiving care, and **shall** ensure compliance as required by appropriate regulatory and accrediting agencies.

2. Health professionals using telehealth **shall** be cognizant of establishment of a provider-patient relationship within the context of a telehealth encounter, whether interactive, store-and-forward or other mode of communication/interaction is used, and they **shall** proceed accordingly with an evidence-based standard of care. Health professionals should refer to existing specialty guidelines to determine whether specific definitions of "patient-provider relationship" and/or "encounter" exist.

3. Health professionals providing telehealth services **shall** have the necessary education, training/orientation, licensure, and ongoing continuing education/professional development, in order to ensure the necessary knowledge and competencies for safe provision of quality health services in their specialty area.

4. Healthcare professionals providing telehealth services should insure that workspaces are secure, private, reasonably soundproof, and have a lockable door to prevent unexpected entry. Efforts **shall** be made to ensure privacy so provider discussion cannot be overheard by others outside of the room where the service is provided. If other people are in either the patient of the professional's room, both the professional and patient **shall** be made aware of the other person and agree to their presence.

Clinical Guidelines

1. The health professionals providing care via telehealth **shall** be aware of pertinent professional discipline guidelines and standards that **shall** be upheld in the telehealth encounter, with consideration of the specific context, location, timing, and services delivered to the patient.

2. Health professionals **shall** be guided by professional discipline and national existing practice guidelines when practicing via telehealth, and any modifications to specialty-specific clinical practice guidelines for the telehealth setting **shall** ensure that clinical requirements specific to the discipline are maintained.

3. Means for verification of provider and patient identity **shall** be implemented. For services with the patient at a healthcare institution, the verification of both professional and patient identity may occur at the host facility. When providing professional services to a patient in a setting without an immediately available health professional (e.g., the patient's home), the telehealth provider **shall** provide the patient (or legal representative) with his or her qualifications, licensure information, and, when applicable, registration number (e,g., National Provider Identification). The health professional **shall** also provide a location for verifying this information. Patients **shall** provide their full name, date of birth, and contact information including telephone, email, and mail contact information prior to the initial encounter. Professionals may ask patients to verify their identity more formally by providing a government issued photo ID. In cases where there is an existing established relationship between patient and healthcare professional and this documentation already exists, this process may be omitted.

4. The organization and health professionals **shall** document (e.g., in the electronic health record) provider (e.g., clinical association, town, state) and patient location, as required for the appropriate payment of services. However, it is not necessary for the health care providers to reveal their specific location to the patient, especially if a provider is located at home at the time of service. Verification of location is critical for complying with relevant licensing laws in the jurisdiction where the provider is physically located when providing the care, as well as where patient is located when receiving care. This information is also needed if an emergency arises and a management protocol must be implemented.

5. The organization and health professionals **shall** review with the patient expectations regarding additional contact between patient and provider (e.g., whether or not the provider will be available for phone or electronic contact between sessions and the conditions under which such contact is appropriate). This review should also include a discussion of emergency management between sessions.

6. Health professionals providing telehealth services **shall** be familiar with the use of any devices and software employed in delivering care over distances. This may include receiving specific training in such devices and software prior to providing patient services.

7. The professional should be familiar with local in-person health resources and travel requirements and should exercise clinical judgment to make a referral for additional health services when appropriate. The professional should also know the preferred healthcare system for the patient's insurance to avoid unnecessary financial strain for the patient.

8. When a professional sees a patient via personal computer and/or mobile device outside the patient's home (e.g., local facility, community-based outpatient facility, school site,

library) or other facility where dedicated staff might be present, the professional should become familiar with emergency procedures. When the patient is in a setting without clinical staff, the professional may request the contact information of a family or community member who could be called upon for support in the case of an emergency. This person, called the "Patient Support Person" **shall** be selected by the patient or legal guardian prior to any telehealth services. In some cases, the facility will not have procedures in place. In cases where emergency procedures are not in place, the professional should coordinate with the clinical/Patient Support Person to establish basic procedures. The basic procedures may include: 1) identifying local emergency resources and phone numbers; 2) becoming familiar with location of nearest hospital emergency room capable of managing emergencies; and 3) having patient's family / support contact information. The professional may also learn the chosen emergency response system's average response time (e.g., 30 minutes vs. 5 hours) and the contact information for other local or regional professional associations, such as the city, county, state, or provincial.

9. In case of medication side effects, elevation in symptoms, and/or issues related to medication noncompliance, the professional should be familiar with the patient's prescription and medication dispensation options. Similarly, when prescribing, the clinician should be aware of the availability of specific medications in the geographic location of the patient. If services are provided in a setting where a professional is not immediately available, the patient might be at risk if there is an acute change in his or her medical and/or mental health condition. Therefore, the professional should be familiar with whom the patient is receiving other medical services.

10. Professionals **shall** be culturally competent to deliver services to the populations that they serve. Examples of factors to consider include awareness of the client's language, ethnicity, race, age, gender, sexual orientation, geographical location, socioeconomic, and cultural backgrounds. Health professionals are encouraged to use online resources to learn about the community in which the patient resides including any recent significant events and cultural mores of that community.

Technical Guidelines

Communication Modes & Applications

All efforts **shall** be taken to use communication modes and applications that have appropriate verification, confidentiality, and security parameters necessary to be utilized properly. Software platforms should not be used when they include social media functions that notify users when anyone on a contact list logs on. When there are situations where multiple participants at different sites (i.e., more than 2) are involved such as with virtual care team conferences or two

consultants interacting with the patient simultaneously, the guidelines apply to all participating sites.

Devices & Equipment

Both the professional and patient site should when available use high quality cameras (video and/or still as clinically appropriate for the intended application), audio, and related data capture and transmission equipment that is appropriate for the telehealth clinical encounter, and which meet any existing practice-specific guidelines. Devices **shall** have up-to-date security software per the manufacturer's recommendations. Health professionals/organizations should use device management software to provide consistent oversight of applications, device and data configuration and security. In the event of a technology fault or failure the organization and health professionals **shall** have a backup plan in place that outlines an alternate method of communication between sites. The plan **shall** be communicated to the patient or referring provider prior to commencement of the initial treatment encounter, and it may also be included in the general emergency management protocol. The professional should review the technology backup plan on a routine basis.

In addition, organizations **shall**:

1. Ensure that equipment sufficient to support diagnostic needs is available and functioning properly at the time of facility encounters.

2. Have strategies in place to address environmental elements of care necessary for safe use of telehealth equipment.

3. Comply with all relevant laws, regulations, and codes for technology and technical safety.

4. Have infection control policies and procedures in place for the use of telehealth equipment and patient peripherals that comply with organizational, legal, and regulatory requirements.

5. Have processes in place to ensure the safety and effectiveness of equipment through on-going maintenance.

6. Meet required published technical standards and regulations (e.g., Food and Drug Administration) for safety and efficacy for devices that interact with patients or are integral to the diagnostic capabilities of the practitioner when and where applicable.

Connectivity for Real-Time Interactive Encounters

1. Healthcare processes that provide one-way or two-way live video services through consumer devices that use internet-based video conferencing software programs should provide such services at a bandwidth of at least 384 Kbps in each of the downlink and uplink directions. Such services should provide a minimum of 640 x 480 resolution at 30 frames per second. In some circumstances, as determined by the health professional, lower or higher bandwidth and frame rate may be used. Depending on the service provided, higher bandwidth speeds may be needed, as determined by the health professional. Because different technologies provide different video quality results at the same bandwidth, each end point **shall** use bandwidth sufficient to achieve at least the minimum quality shown above during normal operation.

2. Where practical, providers may recommend preferred video conferencing software and/or video and audio hardware to the patient, as well as providing any relevant software and/or hardware configuration considerations.

3. The provider and/or patient may use link test tools (e.g., bandwidth test) to pre-test the connection before starting their session to ensure the link has sufficient quality to support the session.

4. Whenever possible, each party should use the most reliable connection method to access the Internet as determined by the health professional or IT team. [10]

5. The videoconference software should be able to adapt to changing bandwidth environments without losing the connection. Organizations **shall** have appropriate redundant systems in place that ensure availability of the data transmission infrastructure for critical connectivity.

Privacy

1. Audio, video, and all other data transmission **shall** be secure through the use of encryption (at least on the side of the healthcare professional) that meets recognized standards.

2. Individuals in charge of technology should familiarize themselves with the technologies available regarding computer and mobile device security, and should help educate the patient with respect to such issues as privacy and security options. Videoconferencing privacy features should be available to both the provider and patient. Privacy features should include audio muting, video muting, and the ability to easily change from public to private audio mode.

3. When the patient and/or provider use a mobile device, special attention should be placed on the relative privacy of information being communicated over such technology.

4. Providers should ensure that access to any patient contact information stored on any device is adequately restricted. Devices **shall** require a passphrase or equivalent security feature before the device can be accessed. If multi-factor authentication is available, it should be used. Devices should be configured to utilize an inactivity timeout function that requires a passphrase or re-authentication to access the device after the timeout threshold has been exceeded. This timeout should not exceed 15 minutes. Mobile devices should be kept in the possession of the provider when traveling or in an uncontrolled environment. Unauthorized persons **shall not** be allowed access to sensitive information stored on any device, or use the device to access sensitive applications or network resources. Providers should have the capability to remotely disable or wipe their mobile device in the event it is lost or stolen. Providers and organizations may consider establishing guidelines for periodic purging or deletion of telehealth related files from mobile devices.

5. Videoconferencing software **shall** allow only a single session to be opened, although the session may include more than two sites/participants. If there is an attempt to open a second session, the system **shall** either log off the first session or block the second session from being opened. Session logs stored in third party locations (i.e., not on patients' or providers' access device) **shall** be secure. Access to these session logs **shall** only be granted to authorized users. This does not preclude the use of multiple cameras during the same session (e.g., videoconferencing camera plus hand-held examination camera).

6. Protected health information and other confidential data **shall** only be backed up to or stored on secure data storage locations. Cloud services unable to achieve compliance **shall not** be used for personal health information (PHI) or confidential data. Professionals may monitor whether any of the transmission data is intentionally or inadvertently stored on the patient's or professional's computer hard drive. If so, the hard drive of the provider should use whole disk encryption as providing acceptable levels of security to ensure security and privacy.

7. Professionals should provide information to patients about the potential for inadvertently storing data and patient information, and they should provide guidance about how best to protect privacy. Professionals and patients **shall** discuss any intention to record services, how this information will be stored, and how privacy will be protected.

8. When organizations and health professionals make recordings of telehealth encounters, they should be encrypted for maximum security. Access to the recordings **shall** only be granted to authorized users and should be streamed to protect from accidental or unauthorized file sharing and/or transfer. The professional may also want to discuss his or her policy with regards to the patient sharing portions of this information with the general public. Written agreements pertaining to this issue can protect both the patient

and the professional. If services are recorded, the recordings **shall** be stored in a secured location. Access to the recordings **shall** only be granted to authorized users.

Appendix

References

1. National Initiative for TeleHealth Guidelines: Environmental Scan of Organizational, Technology, Clinical and Human Resource Issues. RW Pong, JC Hogenbirk, K Byrne, L Liboiron-Grenier, P Jennett, M Yeo, J Finley, D Reid, C Szpilfogel, S Heath, P Brockway, TCradduck. April 30, 2003. http://www.cranhr.ca/pdf/NIFTEEnvironmentalScan-ExecutiveSummary-May72003.pdf. Last accessed October 14, 2013.

2. Telehealth Service Code of Practice for Europe. http://www.telehealthcode.eu/. Last accessed February 28, 2014.

3. American Telehealth Association. http://www.americantelemed.org/practice/nomenclature Last accessed October 14, 2013.

4. Health Insurance Portability and Accountability Act (HIPAA). http://www.hhs.gov/ocr/privacy/. Last accessed February 28, 2014.
5. Patient Safety and Quality Improvement Act of 2005. http://www.hhs.gov/ocr/privacy/. Last accessed February 28, 2014.
6. HeathIT.gov State Licensing Issues Related to Telehealth. http://www.healthit.gov/providers-professionals/faqs/are-there-state-licensing-issues-related-telehealth. Last accessed February 28, 2014.
7. Federation of State Medical Boards Telehealth Overview. http://www.fsmb.org/pdf/grpol_telehealth_licensure.pdf. Last accessed February 28, 2014.
8. Department of Health and Human Services Centers for Medicare & Medicaid Services Medicare Learning Network. http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/telehealthsrvcsfctsht.pdf. Last accessed February 28, 2014.
9. Medicaid.gov Telehealth. http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Delivery-Systems/Telehealth.html. Last accessed February 28, 2014.
10. mHealth Laws and Regulations. http://telehealthpolicy.us/mhealth-laws-and-regulations. Last accessed February 28, 2014.