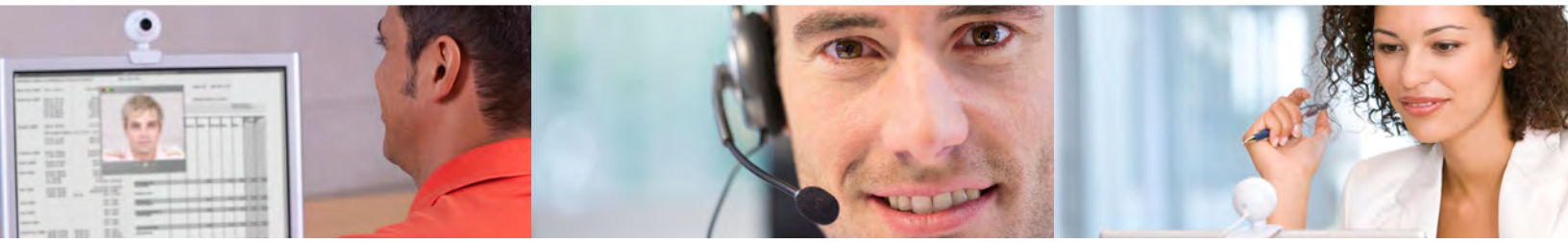
WiscRisk
A Quarterly Publication of the State of Wisconsin
Injured Patients & Families Compensation Fund



DESIGNING A RISK AND COMPLIANCE PROGRAM FOR TELEMEDICINE AND TELEHEALTH SERVICES

By Donna Jennings, RRT, MBA, CPHQ, CPHRM, Senior Consultant, Oliver Wyman Clinical Solutions and Nina M. Antoniotti, RN, MBS, PhD, Director of TeleHealth Business, Marshfield Health System

Telemedicine can be defined as the delivery of health care services to patients where the patient and the practitioner are not physically present in the same location and are using telecommunications to share health information. Most often telemedicine uses interactive two-way audio and video, as well as store-and-forward programs[1] to provide care and health information to patients.

This article seeks to provide a global understanding of telemedicine and telehealth services as well as highlight common barriers and risk management issues associated with implementing a "telemedicine or telehealth" program in their facilities. The document contains tools, resources and risk management strategies that will support the development of a sound Risk Management and Compliance Plan for telemedicine and telehealth services.

The terms telemedicine and telehealth are often used interchangeably, but commonly telemedicine refers to a live, interactive visit between a clinician and a patient, typically for billable services. Telehealth is a term reserved as a broad umbrella under which the many uses of distant virtual care technologies that link patients to providers are used, such as remote monitoring, patient portals, store-and-forward case files, etc. mobile health (m-health) is a term that is used to describe interactions in the health care arena that are done from mobile devices such as a laptop, tablet, or smart phone and typically involve the use of apps.

Some states interchange or alternate the terms "telemedicine" and/or "telehealth." In some states, both terms are explicitly defined in law and regulations and in other states "telehealth" is used to reflect a broader definition of services while "telemedicine" is used mainly to define delivery of medical

1 Store-and-Forward Telehealth involves the acquisition and storing of clinical information (e.g. data, image, sound, video) that is then forwarded to (or retrieved by) another site for clinical evaluation.

services[2]. Wisconsin law interchanges the terms "telemedicine and telehealth" in its definition. Medicaid regulatory language reads as follows: "*Telemedicine services (also known as "Telehealth") are services provided from a remote location using a combination of interactive video, audio, and externally acquired images through a networking environment between a member (i.e., the originating site) and a Medicaid-enrolled provider at a remote location (i.e., distant site). The services must be of sufficient audio and visual fidelity and clarity as to be functionally equivalent to a face-to-face contact. Telemedicine services do not include telephone conversations or Internet-based communication between providers or between providers and members*[3].

Regulatory Oversight

There are several regulatory agencies providing programming and billing requirements for telemedicine services. The inconsistencies among state and federal regulations require a thorough review of payer policies, program requirements (such as in-person requirements, or use of mobile apps), and licensure and scope of practice. Medicare and state Medicaid, as well a private payer payment policies should be evaluated to ensure proper billing and coding and the avoidance of fraudulent claims to government payers. Risk and Compliance staff should be a part of the operational team that reviews all legal and regulatory requirements as telemedicine programs are put into place. The most prevalent agencies currently providing guidance and mandates to facilities desiring to implement telemedicine programs include:

- Food and Drug Administration ("FDA")
  - Regulates medical equipment and software used in telehealth technology such as equipment or software intended for use in the diagnosis or treatment of a disease or other condition
  - Currently, a government-led task force including the FDA, National Institutes of Health and the Department of Health and Human Services is crafting an action plan so that by 2017, mHealth solutions will routinely be available as part of "best practices" for national medical care and treatment[4]
- Centers for Medicare & Medicaid Services ("CMS")
  - Regulates credentialing of practitioners providing telemedicine services; all providers must be credentialed as if they worked onsite when required by the regulatory language or the patient site.
  - Hospital governing body retains overall responsibility for credentialing and privileging decisions
- State health codes, pharmacy and medical boards, etc.
  - States may require the practitioner to be privileged at the site from where he/she is providing services
  - Some states require a practitioner to be fully licensed in the state where the patient receiving services is located; others offer a telemedicine license, license portability, or a licensure compact for practitioners desiring to be licensed in the state in which the patient lives and is receiving services.
  - A licensure compact for physician license portability has been proposed and is being reviewed by several states. The portability requirement has several restrictions for licensing and requires states to pay a fee to a governing board to participate. Federal State Medical Board (FSMB): http://www.fiercehealthit.com/story/compact-aims-ease-licensing-telemedicine-out-state-care/2014-09-08.

HIPAA, Privacy and Security

Healthcare providers participating in telemedicine have the same obligation of responsibility for the privacy and security of patient information as those providing face-to-face care, and they must abide by the rules of HIPAA and the HITECH Act[5]. Hospitals and physicians should also be wary of unencrypted communication platforms such as Skype or Google Talk, which do not allow for providers to protect against breaches[6].

Risk Management Strategies

- Encryption technology should be extended to portable devices and removable storage media
- Safeguard patient's data during transmission by utilizing established facility privacy and information technology security measures (authentication, wireless encryption, patient identification, and data control, data tracking and a protected access system).
- Request vendor protocols for "accuracy of information transfers" and HIPAA compliance documents
- Mandatory HIPAA training for all staff with a specific training module dedicated to telemedicine providers.

Informed Consent

There are few inherent risks associated with telemedicine encounters. The majority of case law to date is under the umbrella of missed diagnoses in teleradiology, which does not apply to live interactive clinical visits. There are several cases that have been brought forward by patients who were not offered telemedicine access to care and had a bad outcome. Provider delays, potential equipment failures and the possibility of security breaches are some of the very uncommon possible

2 Telemedicine Definition, Medicaid. http://www.medicaid.gov/Medicaid-CHIP-Program-Information/By-Topics/Deliv¬ery-Systems/Telemedicine.html.
3 WI Medicaid Program Telemedicine/Telehealth Definition. WI Forward Health, Wisconsin Medicaid Provider Manual, Physician, p. 135 (Jan. 31, 2014)
4 Telemedicine and International Telemedicine: Risks That May Ensue. ASHRM Conference 2013
5 ibid.
6 ibid.

risks, but these stated risks are no different than in-person care. There is mixed opinion on the need for informed consent. Most organizations do not get informed consent as corporate counsel views telemedicine encounters as the same as in-person. Other organizations require informed consent due to state law, or research holdovers.

Risk Management Strategies

- Add a telemedicine informational section to your current facility-wide informed consent policies and procedures
- Design a general telemedicine information pamphlet to be given/mailed to all patients using telemedicine that includes a contact number for questions or concerns.
- Review general admission ("Consent to Treat") and any other pertinent consent documents to assure that updates include patient authorization for services via telemedicine.

Written Agreements and Contracting

Prior to offering telemedicine services, providers commonly need to enter into a business affiliate agreement with other health care institutions who will be providing or receiving services, or networks supporting the delivery of care via telemedicine. The terms of such agreements will vary depending upon the type of entity providing the services and the services to be delivered. At a minimum, the agreements shall include HIPAA compliance statements, credentialing and privileging processes, federal compliance sections, and equipment purchase and maintenance terms.

Risk Management Strategies

- Refer to the Risk Management Resource section for a summary of Medicare's written agreement criteria for the provision of telemedicine services. The links provide direct access to the Center for Telehealth and e-Health Law (Ctel) website where sample written agreements are readily available for use. (www.ctel.org)[7]
- Contracting with Telemedicine Providers and Vendors should include the following requirements for Originating Site and Distant Site Entities[8]:
- Adherence to state, local and federal regulations and guidelines
- HIPAA Privacy and Security requirements
- Executed Business Associate agreement
- Adverse event reporting and Monitoring of Key Performance Metrics
- Medical Director Oversight and Duties

Credentialing and Privileging

The Centers for Medicare and Medicaid Services' (CMS) rule on credentialing and privileging was final July 2011. This final rule established a process for originating site hospitals (location of the patient) to rely on the credentialing and privileging of the distant site location (location of the specialist) for telemedicine/tele-health practitioners (i.e. Credentialing by "Proxy")[9] [10] Although credentialing by proxy improves efficiencies, some providers have chosen to continue with full credentialing and privileging process as a risk mitigation strategy. The responsibility of appropriately credentialing and privileging clinicians belongs with the patient (originating) site.

Risk Management Strategies

- Ensure that allied providers who use telemedicine, practice within their scope of practice with regards to supervision requirements
- Review credentialing policies and procedures of distant facility to ensure that CMS's Conditions of Participation (CoP) are met
- Ensure that licensing requirements for practicing across state lines are followed for the state in which the patient receives care
- Establish a Professional Practice Evaluation (OPPE and FPPE) program for Telemedicine providers using compliance, quality and clinical outcome data
- Assure that telemedicine privileges are defined in medical staff policies and bylaws for the originating site

Developing a Telemedicine Risk Management and Compliance Plan

The Risk Management staff should work with the telemedicine clinical implementation team, Legal and Compliance, to fully vet the telemedicine program to ensure compliance with state and federal, as well as scope of practice requirements for practicing via telemedicine. The Risk Management department should participate in the review of operational telemedicine policies, procedures and clinical protocols.

The following policies and procedures should already be in place for the organization. They also apply to telemedicine encounters' and need not be changed or amended for telemedicine:

- Patient Education Policy
- HIPAA and Secure Data transmission policy
- Organization security/privacy risk assessment process

7 Center for Tele-health & e-Health Law (Ctel), at www.ctel.org
8 Telemedicine: Risk Management Issues, Telemedicine Credentialing and Privileging: Achieving Compliance with the CMS Final Rule. VantagePoint. 2012 Issue 3. CNA HealthPro
9 Telemedicine: Risk Management Issues, Telemedicine Credentialing and Privileging: Achieving Compliance with the CMS Final Rule. VantagePoint. 2012 Issue 3. CNA HealthPro
10 Centers for Medicare & Medicaid Services (CMS), at www.cms.gov

- Email and website usage policy (Security, Privacy and Breach procedures)
- Physician-patient relationship policy
- Patient abandonment (Define "who owns the patient")
- Medical record documentation requirements
- Process for reviewing Contractual and Vendor arrangements
- Event Reporting Process for Patient Care Services Physician Licensing and Privileging Policies
- Policy on Billing, Coding and Reimbursement
- Inclusion of state and federal telemedicine requirements in bylaws and medical staff policies
- Policy on equipment vetting, selection, training, safety and maintenance
- In addition, specific language should be developed to outline policies and procedures for managing:
- Telemedicine Complaint Management Process – how to get a complaint at a distant site to the consulting site and vice versa
- Telemedicine training modules for provider and staff
- Inclusion of telemedicine services in the Emergency Management and Disaster Contingency Plan to assure non-interruption of services
- Utilize a risk and compliance program checklist for telemedicine program – sample checklists available at the Center for Telehealth & e-Health Law (www.ctel.org)

The risk manager plays a key role in assuring assessments have been completed for existing and evolving healthcare services, including telemedicine initiatives. Telemedicine guidelines, regulatory requirements, state laws, and health plans are constantly changing. These changes demand a close watch and team effort between by Risk Management, Quality and Compliance, Clinical Administration, and Telemedicine Directors and Administrator.

Standards for implementing a telemedicine program are published and available for implementing a regulatory compliant program can be found in the 2014 edition of ATA's Core Operational Guidelines for telemedicine ATA Guideline Link[11].

11 (http://www.americantelemed.org/docs/default-source/standards/core-operational-guidelines-for-telehealth-services.pdf?sfvrsn=4).

Additional Telemedicine Resources

Reimbursement

- http://telehealthpolicy.us/state-laws-and-reimbursement-policies
- http://www.amdtelemedicine.com/telemedicine-resources/PrivatePayersByState.html
- http://www.americantelemed.org/docs/default-source/policy/state-telemedicine-policy-matrix.pdf?sfvrsn=44

Telemedicine Prescribing

- http://www.gptrac.org/wp-content/uploads/2011/10/Telemedicine_Prescribing_GPTRC1.pdf

State and Federal Regulatory Compliance

- http://ctel.org/library/resources/
- http://www.americantelemed.org/policy/state-telemedicine-policy#.U76Qg41dXnI

Licensing Updates

- http://www.fiercehealthit.com/story/compact-aims-ease-licensing-telemedicine-out-state-care/2014-09-08
- http://www.healthit.gov/providers-professionals/faqs/are-there-state-licensing-issues-related-telehealth
- http://www.telehealthresourcecenter.org/toolbox-module/credentialing-and-licensing
- http://telehealthpolicy.us/sites/telehealthpolicy.us/files/uploader/FSMB%20Model%20Telemedicine%20Guidelines%20TRC.pdf

Telemedicine and Telehealth Standards and Guidelines

- http://www.americantelemed.org/resources/standards/ata-standards-guidelines#.U76VF41dXnI
- http://www.americantelemed.org/resources/standards/guidelines-from-other-organizations#.U76VVY1dXnI

Telemedicine Consent and Evaluation Sample Forms

- http://www.americantelemed.org/resources/forms#.U76V841dXnJ
- http://www.calhospital.org/post-acute-care

Telehealth Resources:

- http://www.handsontelehealth.com/about
- http://telehealthpolicy.us/telehealth-reimbursement-policy

Medical Malpractice Tele-health/Telemedicine Cases

- http://www.healthlawyers.org/Events/Programs/Materials/Documents/HHS09/kepler_mcginty.pdf

Privacy, HIPAA and Contracting

- http://www.telehealthresourcecenter.org/toolbox-module/legal-issues-privacy-and-contracting-services
- http://hawaii.gov/hhsc/policies-and-procedures/Telemedicine/TEL%200001_021202_.pdf/

About WiscRisk

WiscRisk is published quarterly and circulated to more than 15,000 healthcare providers statewide. Designed to keep readers informed of trends in liability claims and loss prevention, this publication is prepared by the Risk Management Steering Committee for the Injured Patients and Families Compensation Fund.

Articles published in WiscRisk contain the expressed opinions and experiences of the authors and do not necessarily represent the position of the Injured Patients and Families Compensation Fund. Authors are required to make disclosure of any relevant financial relations, which may be related to the subject matter discussed. Authors have made proper disclosure and have no relevant financial relationships that exist now or in the past 12 months.

Steering Committee Members

Linda Syth
Wisconsin Medical Society

Robert Gribble, MD
Marshfield Clinic

Deborah Ankowicz
University of Wisconsin Hospital and Clinics

Denny Thomas
Ministry Health Care

Reid Olson, MD
Dean Health System

Kathryn Osborne
Frontier School

Mary Beth Schneider, CRNA
Wisconsin Association of Nurse Anesthetists

Support Staff

Andrea Nelson
State of Wisconsin Office of the Commissioner of Insurance

Denise Fitzpatrick, RN, MBA, CPHRM
Oliver Wyman Consulting

Stan Hoffert
Wausau MedMal Management Services