



**RISK
MANAGEMENT
SERIES**

For more information contact

Jacqueline C. Leifer, Esq. or
Melinda G. Murray, Esq.
Feldesman Tucker Leifer Fidell LLP
2001 L Street NW
Washington DC 20036
Telephone: (202) 466-8960
Fax: (202) 293-8103
Email: MMurray@ftlf.com

or

Betsy Vieth
National Association of Community
Health Centers, Inc.
7200 Wisconsin Avenue, Suite 210
Bethesda, Maryland 20814
Telephone: (301) 347-0400
Fax: (301) 347-0459
Email: BVieth@nachc.com

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is published with the understanding that the publisher is not engaged in rendering legal, financial or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The Health Resources and Services Administration, Bureau of Primary Health Care (HRSA/BPHC) supported this publication under Cooperative Agreement Number U30CS00209. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of HRSA/BPHC.

Telemedicine and Health Centers: The Doctor is Online

One are the days when Timmy's courageous dog, Lassie, would go get help if Timmy fell out of a tree on the family farm. Today, Timmy would be helicoptered to a rural hospital or a trauma center where digitized images could be sent across the state or even out-of-state to determine the nature of his injuries. Now the Timmys of this world can be "treated" by physicians across the country and across the world. The ability to access specialists through telemedicine is a predictable consequence of the advances in telecommunications technology and the dramatic increase in access to the Internet and the millions of gigabytes of medical information found there.

"Telemedicine," no longer the dream of visionaries,¹ is defined as the use of electronic communications and information technologies to provide clinical services when participating parties are at different locations.² Telemedicine is the technological equivalent of a home run in terms of the access to high-quality health care it can bring to patients in remote or underserved areas who previously would have had to travel hours, perhaps take off another day or two of work, or not receive the care at all. According to HHS Secretary Michael Leavitt:

Information technology is a pivotal part of transforming our health care system. We are at a critical juncture. Working in close collaboration, the

- 1 In fact, telemedicine has been in use in some form for at least 50 years. In 1955, the Nebraska Psychiatric Institute was one of the first facilities in the country to use closed-circuit television which allowed a two-way link between the Psychiatric Institute and Norfolk State Hospital 112 miles away. The link was used for education and consultations between specialists and general psychiatric practitioners. Then in the early 1960s, the National Aeronautics and Space Administration used telemedicine to monitor the physiological parameters of its astronauts in the spacecraft during its space missions.
- 2 The American Telemedicine Association, "Telemedicine, Telehealth, and Health Information Technology," p. 3, May 2006, www.atmeda.org.

Federal government and private sector can drive changes that will lead to fewer medical errors, lower costs, less hassle, and better care.

“Telehealth” refers more broadly to the same technologies, but is used to provide education, consumer outreach, and other applications. For example, a consumer who logs onto the WebMD site for information about diabetes or medical residents who log onto a lecture at another medical center are both using telehealth services.

This Information Bulletin:

- ◆ Discusses current Federal initiatives to encourage the use of telemedicine and telehealth services;
- ◆ Explores the legal and regulatory issues associated with utilizing such services;
- ◆ Focuses on areas health centers should consider prior to developing and participating in a telemedicine and/or telehealth network; and
- ◆ Provides a “checklist” of precautions to take to avoid (or minimize) potential liability exposures which may arise in the course of using telemedicine and/or telehealth technologies to increase patient access to much needed services.

HOW TELEMEDICINE TECHNOLOGIES DELIVER SERVICES TO PATIENTS

As a preliminary matter, it is important for health centers to understand how telemedicine technologies deliver services to patients. Telemedicine technologies enable the delivery of direct patient care through an integrated network with outlying clinics and health centers linked to tertiary care centers in a hub and spoke fashion.³ Patient care can also be delivered directly to a patient at an ambulatory care site or even provided as a health provider-to-home connection through a single line phone-video system. Indeed, telemedicine can

provide direct patient monitoring links for pacemaker, cardiac or fetal monitoring.

The health provider-patient interaction can occur through a variety of technologies including:

- ◆ Videoconferencing, in which the health care provider and the patient can “see” one another and simultaneously share information;
- ◆ Store and forward imaging, in which the results of a diagnostic test are recorded and sent to a

distant site for later viewing;

- ◆ Streaming media, in which continuous patient vital signs are collected remotely and sent to a monitoring station so that the distant provider can keep track of them on an ongoing basis;
- ◆ Terrestrial and wireless communications; and of course
- ◆ The Internet.⁴

FEDERAL INITIATIVES

The increase in the use of telemedicine services has been bolstered by the Administration’s 2004 e-health initiative which calls for the widespread adoption of interoperable electronic health records within 10 years.

The Office of the National Coordinator for Health Information Technology (ONC) – established within the Department of Health and Human Services (DHHS) to develop a nationwide interoperable health information technology infrastructure to:

- ◆ Improve health care quality
- ◆ Reduce errors
- ◆ Reduce costs and

3 The American Telemedicine Association recently estimated that there were 200 networks involving 3,500 health care institutions in the country. ATA, *Telemedicine, Telehealth & Health Information Technology*, p. 4, May 2006, available at http://www.americantelemed.org/news/policy_issues/HIT_Paper.

4 The Office for the Advancement of Telehealth within the Health Resources and Services Administration provides a “how to” technical guide to setting up a telehealth network from a link on its website at www.hrsa.gov/telehealth. <http://telehealth.muhealth.org/geninfo/TAD.html>.

- ◆ Promote coordination of care and increased choice and competition.⁵

The Office for the Advancement of Telehealth (OAT) — within the Health Resources and Services Administration (HRSA), works with the DHHS Office of the Assistant Secretary for Planning and Evaluation to:

- ◆ Identify privacy, confidentiality, and security concerns unique to telemedicine practice.
- ◆ Lead, coordinate and promote the use of telehealth technologies by administering telehealth grant programs, providing technical assistance, and developing policy initiatives.

To that end, OAT invested over \$250 million in funding from 1989 until 2005 for telehealth/telemedicine demonstration and evaluation projects, including projects in rural and medically underserved areas to improve access and quality of care.

The Department of Agriculture's Rural Development Distance Learning and Telemedicine Loan and Grant Program funded nearly \$21 million in grants, \$9.6 million in loans and an additional \$44 million in grant-loan combinations in FY 2005 to encourage and improve

the use of telecommunications (and, thus, improve access to health care services and education in rural communities) by funding the acquisition and installation of equipment at health care sites, schools, and other locations.⁶

These initiatives are good news for health centers, given the current and future physician shortages in rural and inner city locations, and the difficulties in negotiating referral arrangements with specialists for low-income uninsured and underinsured patients (and even for Medicaid and Medicare beneficiaries), especially in specialties such as cardiology, dermatology, orthopedic surgery, and obstetrics.⁷

LEGAL AND REGULATORY ISSUES

From a legal and regulatory point of view, a number of issues arise when a health center is considering developing or participating in a telemedicine and/or telehealth network.

These issues include:

- ◆ Interstate licensure
- ◆ Fraud and abuse concerns

- ◆ Other potential liability issues (and recommendations for handling them)
- ◆ Privacy and security of patient information
- ◆ Reimbursement for telemedicine services.

Interstate Licensure

To date, there is no single or universal licensure statute for telemedicine arrangements that may cross state (or even country) boundaries. Each state has authority to regulate the health care providers who practice within its borders and, thus, legislates its own requirements and sets up its own mechanism by which clinicians secure a provider license.

State Requirements

Whereas ten years ago, only a few states had provisions that addressed out-of-state telemedicine services in their licensing statutes, as of 2003, thirty three states addressed practice across state lines. Twenty-one of those states require full (in-state) licensure of out-of-state practitioners who provide telemedicine services to in-state patients. Most states, however, have laws allowing practitioners to practice medicine as “consultants,” at the request of, and in consultation with, the referring physician (who is licensed in the state) without obtaining a license. Most of these laws were passed before the rapid expansion of telemedicine technologies and prac-

5 Executive Order 13335, April 27, 2004.

6 HRSA, Telehealth Funding Guide; www.hrsa.gov/telehealth/pubs/funding.htm (last accessed 2/8/07). The Department of Agriculture toolkit is at <http://www.usda.gov/rus/telecom/dlt/dlt.htm>

7 A March 2, 2005 *USA Today*, www.usatoday.com/news/health/2005-03-02-doctor-shortage (accessed 1/31/07) quoted predictions of a national shortfall of 85,000 to 200,000 physicians by 2020.

tice and were not intended to apply to on-going regular telemedicine links,⁸ although some states do permit a specific number of consulting exceptions per year.⁹

State medical boards may also grant licenses by:

- ◆ Recognizing other states' licenses through endorsement, i.e., granting licensure to health professionals in other states that have equivalent standards;
- ◆ Reciprocity, if the states specifically agree to recognize the licenses of the other state(s) without further review of individual credentials; and/or
- ◆ Mutual recognition, when the licensing authorities voluntarily enter into an agreement to accept the policies and processes of a licensee's home state without requiring a license in the second state.

Physician Licensure Portability

As telemedicine has enabled people in underserved areas to gain access to health care, and has made even the most sophisticated specialists accessible virtually anywhere and everywhere, new pressures are being placed on regulators to address the need for physician licensure portability. The current system of licensing within each state tends to be slow, cumbersome, and expensive. The Federation of State Medical Boards (FSMB) crafted a Model Act

in April 1996¹⁰ that calls for an abbreviated, but effective, licensure process for physicians who will not be physically practicing within the state's jurisdiction, but wish to provide telemedicine services to patients residing in the state; to date, no states have adopted the Model Act.

In 1996, FSMB also established a centralized system for Primary Source Verification, which currently contains more than 60,000 physician profiles. Eleven medical licensing boards accept a profile generated by the FSMB's Credentials Verification Service to verify physician credentials.¹¹

While an interstate license would certainly make it easier for a physician to practice (through telemedicine technologies) in particular states, it would require agreement on what the core set of requirements for achieving licensure might be. A national licensure system seems feasible by virtue of the educational and competency standards for state licenses having become fairly standard (*e.g.*, all states require new applicants to graduate from an accredited medical board and to pass the US Medical Licensing Exam).

Centralized Data Management System

In October 2006, OAT awarded grants to FSMB and the National Council of State Boards of Nursing to pilot different models for reducing licensure barriers affecting telehealth, involving the development of a centralized data management system that gives participating state medical boards immediate access to physician credentialing information. The initiative is designed also to facilitate the mobilization of physicians in the event of a natural disaster or terrorism, when medical boards have to share accurate physician information quickly.

Fraud and Abuse Concerns

Health centers may be the recipients of funding for telemedicine technology and maintenance of telemedicine links provided by a hospital or health system or multi-specialty practice. If structured and implemented properly, such contributions should be protected by the Federally-funded health center safe harbor,¹² the primary requirement of which is that the grant or other "remuneration" contribute mean-

8 See generally Joanne Kumekawa, *Legislative Update—Licensure*, www.hrsa.gov/telehealth/pubs/licens.htm.

9 California, Colorado, and Hawaii, for example, allow significant consulting exceptions to licensure. *Id.*

10 www.fsmb.org/pdf/1996_grppol_telemedicine.pdf (accessed 1/31/07).

11 FSMB, *Trends in Physician Regulation, 2006*, www.fsmb.org/pdf/PUB_FSMB_Trends_in_Physician_Regulation_2006.pdf (accessed on 2/1/07.)

12 Section 431(b) of the Medicare Prescription Drug, Improvement and Modernization Act of 2003 ("MMA"); see proposed regulations 42 C.F.R. Part 1001.

ingfully to the health center's ability to increase the availability of or enhance the quality of services provided to the medically underserved population served by the health center. Two Office of Inspector General (OIG) advisory opinions involving contributions to health centers for telemedicine, while not binding precedent on future cases, also support that conclusion.¹³

- ◆ In the first opinion, the OIG advised that a hospital's donation of consultative services, payment of transmission line charges and equipment maintenance, and provision of a consultation room for telemedicine that continued after the expiration of a Federal grant designed to improve access to care would not subject the health center to criminal penalties under the Federal anti-kickback statute.
- ◆ In the second opinion, the OIG advised that a large health system's sponsorship of a consultation service for its school-based health centers likewise would not be a violation of the Federal anti-kickback statute.

Recently, the OIG established a safe harbor for electronic health record

technology (effective October 10, 2006), under which hardware, software, and information technology and training services necessary and used predominantly to create, retrieve, transmit, or receive electronic health records is deemed not to constitute prohibited remuneration in violation of the anti-kickback statute.¹⁴ The distant provider could provide the health center with telemedicine hardware or software provided that:

- ◆ The system is fully interoperable,
- ◆ The receipt of the items or services is not a condition of doing business with the distant provider, and
- ◆ The donation of the goods or services is not based on the volume of the health center's referrals.

To fall within this safe harbor, the parties would have to enter into a formal agreement that specifies the details of the arrangement, including what goods and services are being offered and providing that the health center clinicians retain the freedom to refer patients to whichever provider the clinician determines will best meet the patient's needs.

Other Potential Liability Issues and Recommendations For Handling Them

Potential Liability Issues

Notwithstanding the advantages of telemedicine for both patient and provider, health centers should be aware of the potential liabilities. Areas of potential liability resulting from a health center's use of telemedicine as a means of providing access to distant providers include:

- ◆ Negligence or malpractice;
- ◆ Failure to maintain and support the telemedicine link or network; and
- ◆ E-prescribing.

Negligence and malpractice –

In the traditional delivery model, a physician-patient relationship is established when a patient comes into the office, and the physician agrees to provide a diagnosis or treatment. In order to prove negligence, the patient must demonstrate that the physician failed to exercise the standard of care for the service prevailing in the community.¹⁵

Telemedicine changes the provider-patient relationship model. The actual contact that the provider has with the patient may not be at the point in time that the patient is

13 See Advisory Opinions 99-14 and 04-07. Please note that the first advisory opinion preceded the issuance of the health center safe harbor. Since advisory opinions are limited to their facts, the safe harbor is more useful. However, advisory opinions suggest the OIG's thinking on a particular issue and, in that regard, may be helpful in developing specific arrangements and transactions.

14 Section 1128B(b)(3)(E) of the Social Security Act; 42 C.F.R. Part 1001, 71 Fed. Reg. 45136 (Aug. 6, 2006). There is also an exception under the Stark Law, but since the donation would likely go to, and should go to, the health center and not the physician, it is not relevant to most health centers. 42 C.F.R. Part 411, 71 Fed. Reg. 45140 (Aug. 8, 2006)

15 See Patricia Kuszler, *Telemedicine and Integrated Health Care Delivery: Compounding Malpractice Liability*, Am. J. Law & Med. 1999, 25 (2-3): 297, 309-310.

actually at the health center, particularly if “store and forward”¹⁶ technology is used. Similarly, the distant provider may be unknown to the patient, and there may be multiple “distant” providers so that the patient has no direct contact at all with the person rendering an opinion or recommending treatment.

Practically speaking, the health center may be the only health care provider with whom the patient has direct contact. Although referring a patient to a distant provider via telemedicine could be viewed as no different than physically sending a patient down the street to another provider who is not employed by the health center and whom the patient may not have affirmatively selected, the health center’s liability could be greater in the telemedicine situation because the distant provider in a telemedicine scenario may appear to be under the “apparent authority” of the health center.

Apparent authority is a legal concept under which a court might hold a health center liable for the negligence of a distant provider, because the distant provider “appears” to be under the oversight or control of the health center. Even if the health center disclaims responsibility for the distant provider, such disclaimer may be insufficient to escape liability, because merely providing access to the provider through telemedicine may suggest that:

- ◆ The health center has approved the distant provider; and/or

- ◆ The health center is assuring the quality and appropriateness of the care provided.

The theory of apparent authority has been used by courts to hold hospitals liable in cases where negligent emergency services of a hospital are provided by an independent contractor.¹⁷ As a precaution, health centers should know (and document) the identity and credentials of any distant provider who consults with respect to a health center patient and document the nature of the advice provided.¹⁸ As discussed below, it is advisable for this – and for several other reasons – to have formal agreements in place with distant providers.

The Federal Tort Claims Act may provide adequate professional liability coverage of a health center and its employed providers in a telemedicine encounter. But because an encounter with a distant specialty

provider may not be in scope, a health center should consider either seeking a formal approval from HHS through the deeming process or purchasing commercial professional liability or “gap” insurance. In addition, a specialty physician who is sued by the health center patient for failing to diagnose or properly treat a condition could bring a cross claim against the health center for not diagnosing earlier symptoms or not properly conducting the test that was interpreted by the distant physician. That type of cross-claim against the health center is not covered by the Federal Tort Claims Act.

Despite these liability issues, with the growth of telemedicine and the benefits of access to care, we can imagine a claim alleging that a primary care provider’s failure to provide a specialist by means of a telemedicine consultation could be a breach of the standard of care.¹⁹

16 “Store and forward” refers to a diagnostic test that is forwarded electronically to another provider for interpretation at a later time.

17 See *Darling v. Charleston Community Memorial Hospital*, 211 N.E.2d 253 (Ill. 1965) which was the first case to recognize corporate liability on the part of the hospital, even though it did not employ the physician. Others have recognized a type of “enterprise liability” of a consultant specialist who had very little contact with the patient, but was consulted by a cardiologist about an angiogram. See, e.g., *Bovara v. St. Francis Hospital*, 700 N.E.2d 143 (Ill. App. Ct. 1998.); *Kashishian v. Port*, 481 N.E.2d 277, 278 (Wis. 1992).

18 If this is a one-time or occasional consultation, there may not be an agreement in place and liability for negligence will depend on the allegations and the nature of each person’s responsibility.

19 See Patricia Kuszler, *Telemedicine and Integrated Health Care Delivery: Compounding Malpractice Liability*, 25 Am. J. Law & Med. 297, 316 (1999). See *Washington v. Washington Hospital Center*, 579 A.2d 177 (D.D.C. 1990) where the failure to use an available technology to monitor carbon dioxide during brain surgery was held to violate the standard of care. The American Telemedicine Association is in the process of working clinical and administrative guidelines specific to telemedicine. While telemedicine practitioners have not formally adopted many clinical protocols or technical standards, a few professional associations such as the American Psychological Association, the American Dermatology Association, and the American Nurses Association have posted clinical guidelines to their websites. The American Telemedicine Association, *Telemedicine, Telehealth, and Health Information Technology*, pp. 6-7, May 2006.

Failure to maintain and support the telemedicine link/network – Another area of potential liability arising out of telemedicine is the failure of the technology itself. Since no technological standards of interoperability have been established, there is no clear guidance as to whose responsibility it is to maintain the components of a telehealth system. In addition, much of the information transmitted in telemedicine is “compressed” before it is sent and “decompressed” at the receiving end, which has the potential to distort data, especially images, and can result in a misdiagnosis based on data that has been distorted in transmission.²⁰ The failure of a satellite link when a STAT test is necessary or the network’s failure to have sufficient staff to keep it running at the speed and accuracy that is required by the medical field could also result in exposure.

E-Prescribing – Some states require a face-to face contact in order to write a prescription so that fraud can be avoided. So it may be up to the referring health center physician or nurse practitioner to write the prescription prescribed by the distant practitioner, which could open the health center practitioner to liability if the specialist makes a mistake in dosage and/or type of medication.

Precautions

Generally, we recommend four ways in which health centers can address these liability issues:

- ◆ Credentialing of the distant providers.
- ◆ Purchasing liability insurance.
- ◆ Executing formal agreements with telemedicine providers.
- ◆ Identifying the telemedicine provider in the medical record.

Credentialing of distant providers – Every health center is responsible for ensuring that providers who are rendering care to health center patients, whether in person or via the Internet, have the appropriate credentials. According to the Bureau of Primary Health Care’s Health Center Program Expectations, Policy Information notice (PIN) # 98-23, not only must the health center define standards for assessing the experience and competence of its clinical staff, but credentialing should follow a formal process which includes querying the National Practitioner Data Bank and verifying education and licenses. Credentialing and privileging processes should meet the standards of national accrediting agencies such as the Joint Commission on Accreditation of Health Care Organizations

(JCAHO) and the Accreditation Association for Ambulatory Health Care, Inc., (AAAHC) as well as requirements for coverage under the Federal Tort Claims Act (FTCA).²¹

Effective July 1, 2006, JCAHO published revisions to its Medical Staff standards relating to telemedicine services provided by a licensed independent practitioner (LIP) who has total or shared responsibility for patient care, treatment, and services through a telemedicine link. LIPs who provide official interpretive services through a telemedicine link are credentialed under the contracted services standard (LD 3.50).

The July 2006 standards also introduce the concept of credentialing and privileging “by proxy” in which, under special circumstances, the originating site (where the patient is located) is allowed to accept the credentialing and privileging decisions of the distant site (the site where the practitioner providing the professional service is located). In order to meet this standard (MS 4.120), the health center (as originating site), would retain responsibility for overseeing the safety and quality of services offered to the patients. If the distant site is a JCAHO-accredited organization, then the health center would be able to accept those credentials and be in compliance with JCAHO standards, thus simplifying the credentialing process.

However, the requirements for coverage under the FTCA²² contemplate review and verification of the professional credentials, references, claims history, fitness, professional review organization findings, and

20 Nancy Miller, *Telemedicine Legalities for Physicians in PA*, Physician’s News Digest, pp.3-4, June 1999.

21 PIN # 98-23, p. 19; see also PIN # 2002: *Clarification of Bureau of Primary Health Care Credentialing and Privileging Policy* (July 10, 2002).

22 Health centers and their officers, directors, employees, and certain contractors are eligible for FTCA coverage under the Federally Supported Health Centers Assistance Acts (FSHCAA) of 1992 and 1995.

licensure status of its health professionals by the health center itself.²³ Thus, it is advisable for health centers to personally credential all practitioners who will be providing care to health center patients, including individuals providing telemedicine services.

Purchasing liability insurance – Potential liability problems can also be addressed and mitigated by purchasing appropriate liability insurance. If a health center has been deemed eligible for malpractice liability protection under FTCA, more than likely such coverage would extend to a distant provider only if he or she is an individual with whom the health center contracts for family practice, general internal medicine, general pediatrics, or OB/GYN services. To cover a distant provider practicing in another specialty area, the provider would have to work at least an average of 32 hours per week for the health center.²⁴ Insofar as under the typical telemedicine arrangement, the distant provider would not be able to meet this requirement, the entity or individual who provides a service in a telemedicine encounter should be required to provide evidence of professional liability coverage for those services.²⁵

In addition, the health center may need to secure formal approval of the provisions of telemedicine services through a formal change in scope and/or seeking formal approval for FTCA coverage. We recommend obtaining gap insurance to cover the claim against the off-site doctor, the health center, and/or for

a cross claim asserted by the doctor against the health center—anything incidental to a claim arising out of the telemedicine encounter.

Executing formal agreements with telemedicine providers – The third way to address liability concerns is by establishing relevant terms in a formal written agreement, including:

- ◆ Which party is responsible for the patient's care when the consultant provides advice;
- ◆ Which party is responsible for maintenance of the electronic telemedicine link;
- ◆ If required by state law, a requirement that the distant provider must meet in-state licensure requirements;
- ◆ A requirement that the distant provider must satisfy the health center's credentialing requirements (and notify the health center of any changes);
- ◆ A stipulation that the parties are independent contractors;
- ◆ Which state law will apply if there is inter-state transmission of telemedicine information;
- ◆ HIPAA requirements (as discussed below);
- ◆ Insurance requirements (at least \$1 million per occurrence and \$3 million in the aggregate, by a

company that has a Best rating of A or above, if possible, and no exclusion for telemedicine); and

- ◆ Such other terms as pertinent to the specific arrangement.

Identifying the telemedicine provider in the medical record –

Finally, health center providers should require identification of each provider present or involved in a telemedicine diagnosis or treatment encounter, and document those individuals in the patient's medical record. The health center staff member who is physically with the patient should obtain the names and specialties of the providers who will be performing a test, reviewing the patient's record or test results, or providing recommendations on care, and document their identities in the medical record. In addition, the health center should require telemedicine consultants to promptly provide a copy of the medical record or report they prepare for the encounter.

Privacy and Security of Patient Information

While coordination of care and quality may be enhanced by telemedicine, patient privacy could be compromised.²⁶ There are three areas of vulnerability involving the

23 PIN # 99-08: *Health Centers and the Federal Tort Claims Act*, at p. 2.

24 PIN # 99-08, at pp. 2-3; see also PIN # 2001-11: *Clarification of Policy for Health Centers Deemed Covered under the Federal Tort Claims Act for Medical Malpractice* at p. 2.

25 Health centers should also beware of signing a contract that contains indemnification provisions as FTCA does not cover health centers' indemnification of third parties.

26 Physicians Payment Review Commission, *Annual Report to Congress*, 1995.

confidentiality of health information that is transmitted to a distant site and the security of the electronic transmission.

- ◆ Security of the transmission itself – email is more vulnerable than a landline telephone, for example, and could easily be forwarded to other individuals intentionally or in error.
- ◆ Storage of the information once it reaches the provider's server.
- ◆ Maintenance of the medical record, however stored, and access to the medical information at either site.

While virtually all health care providers know they have to maintain the confidentiality of protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), many may not have a good grasp of the need to comply with HIPAA's Security Rule²⁷, which requires covered entities (including health centers) to ensure the confidentiality, integrity, and availability of electronic protected health information the health center creates, receives, maintains or transmits.²⁸ The Security Rule requires administrative safeguards such as:

- ◆ Risk assessment of potential threats to confidentiality;

- ◆ Risk management through security measures; and
- ◆ A sanctions policy for security violations.

The Security Rule also requires physical safeguards and technical safeguards such as a unique user identification.

It is up to the health center to ensure that patient information that is provided through telemedicine cannot be improperly accessed, by implementing policies and procedures to prevent, detect, contain and correct security violations.²⁹ Steps include:

- ◆ Work closely with IT personnel to determine what kind of information is being transmitted and how it is being transmitted. For example, a photograph of a dermatology lesion sent over a telephone video line may be more secure than a patient history sent by the Internet.
- ◆ Determine vulnerabilities in security procedures and what controls are in place to prevent those security breaches.
- ◆ Install physical and technical security safeguards — such as software passwords, data encryption, digital signatures to

authenticate the sender, backup systems, disaster recovery plan.

Unfortunately, a health center does not have the same degree of control over a distant provider's site, but at minimum, if a formal agreement is executed (as is recommended), the health center can require compliance with HIPAA standards and have a check list of issues to verify with the distant site to make sure security controls are in place.

In addition to establishing a national standard, HIPAA provides that if state law provides a stricter standard than HIPAA, then state law prevails.³⁰ Accordingly, a health center should not only specify in its telemedicine agreement that the distant provider must comply with HIPAA (as well as the health center's policies), but also that it should consult with counsel as to whether the health center's State has a stricter law than HIPAA that would require compliance by the distant provider. If so, that stricter standard should be set forth in the agreement.

Reimbursement for Telemedicine Services

Services rendered via telemedicine are treated differently under the Medicare and Medicaid programs and commercial insurers.³¹

27 45 C.F.R. parts 160, 162, and 164.

28 45 C.F.R. §164.306(a).

29 45 C.F.R. § 164.308(a)(1).

30 See Joanne Kumekawa, "Health Information Privacy Protection: Crisis or Common Sense" *Online Journal of Issues in Nursing*, vol#6, #3, September 30, 2001 available at www.hrsa.gov, hyperlink under "Privacy."

31 See generally Center for Telemedicine Law, *Telemedicine Reimbursement Report*, October 2002, available at <http://www.hrsa.gov/telehealth/pubs/reimbursement.htm>.

Reimbursement under the Medicare Program

For Medicare to make payment to a provider who renders services via telemedicine, the patient must be in an originating site such as a Federally Qualified Health Center (FQHC) that is located in a rural Health Professional Shortage Area (HPSA) or in a county outside a Metropolitan Statistical Area, unless the FQHC is part of a Federal telehealth demonstration project.³² Thus, Medicare would not cover the services of a distant provider in a telemedicine encounter originating in an urban FQHC, although the health center could still bill its services as the originating site.³³

Medicare allows reimbursement for telehealth services that:

- ◆ Are provided by means of interactive audio and video allowing for real time communication;
- ◆ Are furnished by a physician, nurse practitioner, physician's assistant, nurse midwife, clinical nurse specialist, clinical psychologist, clinical social worker, or dietitian to an eligible individual in the same amount as the clinician providing the service would have been paid if the service had been furnished without the use of a telecommunications system;³⁴
- ◆ Have the patient present and participating in the telehealth visit.

The health center, as the originating site, can charge a facility fee of \$22.94 for the interactive consultations described above.

Reimbursement for "store and forward" technology, other than those applications where traditionally a health care practitioner does not require a face-to-face encounter such as radiology, is allowed only in the Alaska and Hawaii demonstration projects.³⁵

Reimbursement under the Medicaid Program

By contrast, the overwhelming reimbursement trend for telemedicine under the Medicaid program is to provide reimbursement if the care involved would be covered if it were provided in-person.³⁶ This includes a variety of interpretive services that use the remote store-and-forward technology, such as

tele-radiology, tele-pathology, EKG interpretation, echocardiography and tele-ultrasound. In addition, as of June 2003, 23 states provided some level of reimbursement for services delivered via telemedicine for interactive consultations to Medicaid recipients.³⁷ The services are coded and billed just like regular in-office services.

Reimbursement by Private Payors

With respect to private payors, many states have enacted legislation providing for telemedicine reimbursement.³⁸ Some insurance programs may cover specific telehealth services, such as behavioral health, while others provide more generally that the services provided by telemedicine will be reimbursed if the same service would be reimbursed when provided in person.

32 Medicare Claims Manual, Transmittal 1798, Sec. 11556, May 16, 2003.

33 See Dena S. Puskin [Director of the Office for the Advancement of Telehealth], *Telemedicine: Follow the Money*, Online Journal of Issues in Nursing, available at www.nursingworld.org/ojin/topic16/tps16_1.htm in which she describes the need for expansion of reimbursement to improve access to specialty services.

34 42 U.S.C. 1395m(m). does this say physician

35 42 U.S.C. 1395 (m)(4)(C), (F); 42 C.F.R. § 414.65; 42 C.F.R. § 410.78. "Medicare Payment of Telemedicine and Telehealth Services, May 15, 2006.

36 Medicaid Reimbursement in the United States, p. 5.

37 American Telemedicine Association, *Medical Assistance and Telehealth: An Evolving Partnership*, available at http://www.atmeda.org/news/policy_issues. These States are Alaska, Arkansas, California, Colorado, Georgia, Illinois, Indiana, Iowa, Kansas, Maine, Michigan, Minnesota, Montana, Nebraska, North Carolina, North Dakota, Oregon, South Dakota, Texas, Utah, Virginia, Wisconsin, and West Virginia.

38 Center for Telemedicine Law, *Telemedicine Reimbursement Report*, p. 7, October 2002, available at <http://www.hrsa.gov/telehealth/pubs/reimbursement.htm>. States that have enacted laws specifying telemedicine as a medical service include Arizona, California, Colorado, Hawaii, Kentucky, Louisiana, Minnesota, Nebraska, Oklahoma, Texas, and Virginia. States with laws concerning reimbursement, specifically, are Massachusetts, New Mexico, New York, and Oregon.

CONCLUSION

Telemedicine fulfills all the goals of the health center program – reasonable access to care, efficiency in service delivery, and the provision of quality care in a timely manner – which when met, can result in reducing the annual cost of care and improving health outcomes.

Attendant costs, such as transportation and the cost of providing emergency care for chronic or primary care problems may also be reduced by establishing telemedicine services. With a shared goal of providing cost effective, high quality comprehensive care, health centers cannot afford to miss out on current and future telemedicine opportunities.

However, as is the case in all segments of the health care industry, new methodologies raise the specter of potential liability exposures. Since the telemedicine field is in its relative infancy, it is difficult to anticipate which exposures will be significant. **In any event, we recommend, in addition to the purchase of private malpractice insurance or securing explicit approval that the health center is protected against claims arising out of telemedicine services discussed above, the following precautions:**

1. **Execute a formal agreement with the distant provider**, including the following key provisions:
 - a. Description of the services.
 - b. The timeframes within which it will be provided (*e.g.*, a STAT diagnostic reading).
 - c. Identification of the individuals who will provide the services and who will be responsible for the patient's care, and relevant credentialing and licensure provisions.
 - d. Statement that the providers are independent contractors and retain independent medical judgment.
 - e. Identification of the provider or entity responsible for installation and maintenance of the electronic link with the telemedicine provider.
 - f. Documentation requirements (*e.g.*, medical records and encounter forms) and the process by which they will be shared.
 - g. Non-discrimination provision.
 - h. Fee schedule (if the health center will compensate the distant provider, and the provider does not bill, for the services rendered and/or technology costs).
 - i. Evidence of professional liability insurance in at least the amounts of \$1/million per claim and \$3 million in the aggregate, by a highly rated company, as well as general liability insurance for matters relating to the link or network itself.
 - j. Compliance with HIPAA's privacy and security provisions for clinical and non-clinical personnel.
 - k. Statement of which State law will apply if the health center and distant provider are in two different States.
 - l. The agreement must be signed by the provider's institution or if a solo clinician, by the clinician him or herself.
 - m. The term and termination provisions for the agreement.
2. **Apply credentialing requirements** to each distant clinician who will provide services and document findings before executing any agreement or authorizing the particular individual to consult.
3. **Ensure privacy and security** by conducting due diligence with respect to the network or methods of transmission of health information to make sure that they are secured. Any outside contractor who is providing IT services and might have access to PHI should sign a business associate agreement.
4. **Document in the same agreement as described above or in a separate agreement** if payment to set up or participate in a telemedicine network is being provided as a donation or community benefit to the health center by a health care provider or vendor. The agreement should provide:
 - a. Protection of patient freedom of choice.
 - b. Non-exclusivity of the clinical services being contracted.
 - c. Assurance that the health care providers retain the right to exercise independent medical judgment.
 - d. Preferably, the donor's commitment (if the donor is a health care provider) to accept referral of health center patients, regardless of their ability to pay or their insurance status.



National Association of Community Health Centers, Inc.[®]

7200 Wisconsin Avenue, Suite 210

Bethesda, MD 20814

Telephone: 301-347-0400

Fax: 301/347-0459

Website: www.nachc.com