Chapter 2
The Law of Telemental Health

Joseph McMenamin

This chapter touches on some of the main legal issues pertinent to the provision of mental healthcare at a distance.

Licensure

Traditionally, the states have regulated healthcare through licensure. Although licensing requirements state to state tend to address common topics (professional education and training, continuing education, ethics, confidentiality, advertising, professional self-governance, etc.), details vary. In no way does a license to practice psychology in State A authorize the bearer to practice in State B; State A is without authority to confer such a privilege. States tend to be rather restrictive in their readings of relevant statutes, partly for quality control—state boards see it as their role to police the profession to protect the public—partly to protect their own licensees, and partly to vindicate state sovereignty.

For a practitioner proposing to offer services across state lines, multistate licensure is a perfectly lawful approach, but it can be costly and cumbersome. Each state has different requirements, and a licensee failing to meet one in a particular state is likely to lose his license there. Keeping up with the requirements is both an administrative headache and a significant financial burden. For a professional who wishes to concentrate on only a couple of states, however, it may be a relatively simple, cost-effective solution.

Portions of this chapter are taken from an unpublished paper prepared in aid of the writer's verbal remarks at the Roundtable on Legal Impediments to Telemedicine, held at the University of Maryland School of Law in Baltimore on 16 April 2010.

J. McMenamin, M.D., J.D. (✉)
10617 Falconbridge Drive, Richmond, VA 23238, USA
e-mail: mcmenamin@medicalawfirm.com

M.M. Maheu et al. (eds.), *Career Paths in Telemental Health*,
DOI 10.1007/978-3-319-23736-7_2

Whether a behavioral health professional wants to practice in a single state or in 50, it is necessary to become acquainted with at least the general contours of the relevant law in each such state. Recognize, though, that laws change. Statutes are enacted, amended, and repealed; new regulations are written; and courts construe legislative language, or previous decisions, sometimes in ways not easily anticipated. Hence, one must not only have a working knowledge of the law in each state where one practices, but one must also make reasonable efforts to stay current with legal requirements as they evolve.

APA published a 50-state survey of laws pertinent to telepsychology, specifically those most pertinent to licensure, and reportedly current as of October 2013. See http://www.apapracticecentral.org/update/2013/10-24/telepsychology-review.aspx. For each state, the survey specifies whether there are telehealth or telepsychology statutes or regulations, whether the practice of psychology is defined to include distance care specifically, whether there is a telehealth coverage mandate, what provisions exist for temporary or guest practice, and what penalties can be imposed for practicing psychology without a license. Some states are plainly more amenable to accommodating out-of-state practitioners than others. With the law in flux, full licensure is still the safest course, except in special circumstances. For example, the military and the VA generally recognize a valid license issued by any state in the union. The private practice world is not so accommodating.

In at least one state, the physician disciplinary authority has declared that treatment via the Internet or over the phone will be held to the same standard as is applied in traditional face-to-face settings (Illinois Medical Disciplinary Board, "Guidelines for the Appropriate Use of Internet/Telephonic Communication in Medical Practice" (2003), cited in John D. Blum, "Internet Medicine and the Evolving Status of the Physician-Patient Relationship," 24 *J. Legal Med.* 413, 445 (2003)). In some states, legislation now provides that, at least as to physicians, the standard of care at a distance is to be the same as that of care in person. See, e.g., Colo. Rev. Stat. § 10-16-123(2), Haw. Rev. Stat. § 453-1.3(d), and 22 Tex. Admin. Code § 174.8(b). Although these authorities govern the practices of physicians, and not of psychologists, they are nevertheless instructive. Our legal system reasons by analogy, and there is a good possibility that boards focused on other branches of the healing arts may be influenced by these and similar legal developments.

For better and for worse, we will likely see some, perhaps substantial, erosion of the power and influence of State Boards in the future. Numerous proposals are pending to create a system similar to that for drivers' licenses, or to create a federal licensing system, or to expand reciprocating arrangements, or to invent a mechanism to license those whose work is limited to distance care. FSMB has developed an Interstate Medical Licensure Compact (http://www.licenseportability.org), effectively a contract between states, which in some particulars resembles the Compact the nurses have had for years (https://www.ncsbn.org/nlc.htm). Counselors have been working toward licensure portability in their 20/20 project. See http://www.counseling.org/knowledge-center/20-20-a-vision-for-the-future-of-counseling/statement-of-principles. In February 2015, the Board of Directors of the Association of State and Provincial Psychology Boards (ASPPB) introduced the Psychology

Interjurisdictional Compact (PSYPACT), designed to facilitate telehealth as well as temporary in-person psychology practice across jurisdictional boundaries (http://www.asppb.net/news/217917/Psychology-Interjurisdictional-Compact-PSYPACT-Announced.htm). As with the compacts developed by other health disciplines, this one requires buy-in from state legislatures. It sets up a Psychology Interjurisdictional Compact Commission, responsible for articulating the rules governing cross-border psychology practice. To practice in a state other than her own, the psychologist must among other things subject herself to the Board in the patient's state, obtain a certificate called an "E. Passport" to be further defined when the Commission is in place, and comply with any other Commission rules.

It is difficult to predict what the final form of licensing will be in a country as large and diverse as ours. Increasingly, however, the emphasis on state borders will be seen as an anachronism. It will grow easier to provide services not only where you hang your hat but where you send your electrons. Over time, that will probably also be true of international practice, as to some extent is already true in the EU, for example. If seven states enact the PSYPACT, it will become valid for practitioners in those states. As of this writing, however, that has not yet occurred.

For now, then, caution is the watchword. State boards have plenary power over a practitioner's license. The best course continues to be to obtain and maintain a license in each state where your patients live. Doing so entails expense, administrative chores, complying with varying continuing education requirements, and, of course, subjecting yourself to the jurisdiction of a board that may be far from home. The alternatives, however, are worse.

A California patient asked an online pharmacy for a refill of fluoxetine, prescribed to manage his depression. Identifying himself as a California resident, the patient filled out an online form, eliciting answers to questions pertinent to medical history, and sent it to a pharmacy in cyberspace. The Internet pharmacy sent the request, and the form, to a server in Texas, which relayed the documentation to Christian Hageseth, MD, a physician licensed and working in Colorado. On the basis of the information submitted, Dr. Hageseth concluded the refill was indicated and sent a prescription back to the Texas server, which in turn sent it to a bricks-and-mortar pharmacy in Mississippi. That pharmacy shipped the actual product to the patient, who died a suicide 2 months later from carbon monoxide poisoning. Although the patient had fluoxetine on board at the time, there was no evidence the drug caused the death; the patient was also inebriated. Finding that there had been no in-person evaluation, the California Board of Medicine concluded that between Dr. Hageseth and the patient, a true doctor–patient relationship had not been established, so it referred the case for prosecution to the state authorities. California took the position that Dr. Hageseth had engaged in the unauthorized practice of medicine there, a felony under § 2052 of the California Business and Professions Code. Dr. Hageseth had never been present in California, nor had he sought patients there. Moreover, another professional, under a separate license, actually filled the script. Dr. Hageseth therefore denied that California had jurisdiction. The California Courts of Appeal, however, held that California authorities could cross state lines to pursue criminal charges against the defendant (*Hageseth v. Superior Court*, 150 Cal.

App. 4th 1399, 59 Cal. Rptr.3d 385 (2007)). Dr. Hageseth was sentenced to 9 months in jail, which he was permitted to serve in Colorado. He also was ordered to pay $4200 to reimburse the California Medical Board for investigation costs.

There do not appear to be any published cases in which a psychologist licensed in one state was criminally prosecuted for caring for a patient electronically in another state. Moreover, the law in California is just that: the law of a single state, not of all 50. *Hageseth*, though, remains instructive. As noted, courts often reason by analogy, and at least until the law changes appreciably, mental health professionals should go to school on Dr. Hageseth's experience.

In a more recent case, the Oklahoma Medical Board disciplined a pain physician, mainly for what it saw as excessively liberal prescribing of controlled substances. The board also sanctioned the licensee, however, for using Skype to communicate with patients, because that approach failed to protect privacy, and for failing to keep adequate records and to perform proper examinations (*State of Oklahoma ex rel. Oklahoma Board of Medical Licensure and Supervision v. Thomas Edward Trow, M.D.*, License No. 10255, case No. 11-11-4439 (12 September 2013). Although this, too, was a medical case, the board's concerns about privacy and record-keeping are not peculiar to physicians.

Privacy

The protection of patient/client privacy is among the best-established obligations of healthcare professionals, dating at least to the time of Hippocrates. In no branch of the healing arts is privacy more important than it is in mental health, concerned as it is with the patient's most sensitive and personal information. The duty to protect patient privacy is reflected in statutes, regulations, and case law, and it applies regardless whether care is provided in-person or at a distance.

By no means can traditional paper-based records guarantee privacy. In telehealth, however, data move from one place to another by electronic means vulnerable to mishap or to intentional invasion. And with so many health professionals now enthusiastically utilizing a wide array of mobile devices and with the continual blurring of the line between our personal and professional lives, the risks of inadvertent disclosures are high and increasing. Scarcely a week goes by without some news report of another breach of healthcare privacy.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), gave rise to the privacy rule, 45 CFR Part 160, and to the security rule, Subparts A and E of Part 164. HIPAA was enacted primarily to permit workers switching jobs to transfer and continue health insurance coverage.

Its elaborate array of rules to protect health information privacy, however, is what HIPAA is best known for. These rules were developed in large part to allay the understandable misgivings of patients fearing that, with the increasing influence of third-party payers, the waning authority of healthcare professionals, the digitization of data of all kinds, and the depersonalization of what used to be the intensely personal exchange between treater and patient, confidence that privacy will be protected was no longer justified.

HIPAA applies only to covered entities (CEs) and business associates (BAs), defined below. For CEs, the HIPAA Privacy and Security Rules govern healthcare records, including, of course, mental healthcare records, and they apply to distance care just as they do to in-person care. As HHS puts it, "the HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information…[It] requires appropriate safeguards to protect the privacy of personal health information ["PHI"], and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections" (http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/). The HIPAA Privacy and Security Rule requires CEs and BAs acting on their behalf to implement administrative, physical, and technical safeguards if engaged in the transmission or storage of PHI. 45 C.F.R. §§ 164.302–318. See http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

Health insurers, healthcare clearinghouses, and healthcare providers who transmit information in electronic form in connection with a transaction governed by an HHS standard are all CEs. "BA" is a broad term and includes entities needing routine access to the CE's PHI to provide data transmission services to it,[1] entities offering personal health records on a CE's behalf, subcontractors (other than mere conduits) of BAs handling PHI for it, and anyone who creates, receives, maintains, or transmits PHI on behalf of a CE (including entities storing electronic PHI). The list of affected BAs may include vendors, contractors, or consultants, such as those providing professional services, e.g., lawyers, accountants, marketers, and software vendors. Under HIPAA, a CE engaging a BA must enter into a contract with the BA, a "business associate agreement" (BAA), imposing on the BA by contract substantially the same obligations the CE shoulders by operation of law. Under the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), BAs are obliged to protect PHI just as CEs are, not just because through BAAs they are contractually bound to do so, but directly under federal law. See 45 C.F.R. § 160.103; 42 USC § 17921(2).

Mental health professionals in particular should remember that patients who pay for services out of pocket can request that their health information not be disclosed to others, including their third-party payers.

[1] The definition of a BA excludes mere conduits of such data, such as telecommunications concerns and Internet carriers. The HITECH Act defines a "conduit" as an entity that transports information, but does not access it except on a random or infrequent basis as necessary to perform the transportation services.

The Final Omnibus Rule

The HIPAA Omnibus Rule (Final Rule), 78 (17) Fed. Reg. 5566-5702, published by HHS on 25 January 2013 pursuant to the Genetic Information Nondiscrimination Act of 2008 (GINA), Pub.L. 110–233, 122 Stat. 881, and to the HITECH Act, 42 USC §§ 17931–39, imposed a compliance deadline of 23 September 2013 on all BAAs entered into after 25 January 2013. All BAAs entered into before then had to be updated and brought into compliance by 23 September 2014. The Final Rule made the legal requirements for PHI privacy and security even more onerous than they were before.

By changing the definition of a breach, the Final Rule lowered the threshold for a finding of liability, simultaneously shifting the burden of proof from the government to the accused. Originally, a breach was defined to mean a compromise of the security or privacy of PHI that posed significant risk of financial, reputational, or other harm to an individual—the so-called "harm" standard. The Final Rule, however, abandoned that standard. A breach is now defined as "impermissible use or disclosure of PHI." Such a use or disclosure "is presumed to be a breach unless an entity demonstrates and documents a low probability PHI was compromised." To show breach, patients need no longer prove "harm"; they need but show unauthorized viewing of patient records, without more.

The Final Rule expands the definition of BA to include health information organizations, e-prescribing gateways, certain personal health record (PHR) providers, patient safety organizations, data transmission service providers with access to PHI, and contractors handling PHI. BA liabilities for HIPAA infractions are substantially identical to those to which covered entities themselves are vulnerable. The Final Rule also provides that a contract between a BA and its subcontractor is required; it must be as stringent as a BAA. Broader exposure for BAs is not tantamount to diminished risk for CEs; they remain liable for their own breaches, just as they were before the Final Rule was promulgated.

The Final Rule also imposes new notification rules triggered when breaches are discovered. Within 60 days of such discovery, CEs (or, under a BAA, the BA) must notify patients in writing, supplying a "brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity (or BA, as applicable)." If the BA is responsible for the breach, it must notify its CE. The CE or the BA must notify the Secretary of HHS of all such breaches annually. When a breach affects more than 500 patients in a given jurisdiction, notification must also be made through prominent media outlets within that jurisdiction and to the Secretary (HHS, Breach Notification Rule, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/). HHS now posts a list of such breaches at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

The HIPAA Final Rule also changes the HIPAA Enforcement Rule to incorporate the HITECH Act's higher civil monetary and criminal penalties. Even in cases when a CE did not know it was committing a HIPAA violation and would not have

known it even by exercising reasonable diligence, civil penalties can range from $100 up to—for willfully negligent breaches—$50,000 per violation with a maximum of $1,500,000 per section violation. Pre-HITECH HIPAA fines, in contrast, were capped at $100 per violation, with an aggregate limit of $25,000.00 per year.

HIPAA provides for severe criminal penalties as well. Under the Final Rule, up to 1 year of imprisonment can be imposed for violations done unknowingly or with reasonable cause to believe they were not violations. A person who knowingly uses, obtains, or discloses individually identifiable health information with the intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm, however, shall be fined not more than $250,000 and/or imprisoned for up to 10 years (42 USC 1320d-6). To understand the gravity of these sanctions, consider the Florida nursing assistant sentenced to 3 years in prison and to a $12,000 fine for stealing and selling, at but meager profit, PHI that included Social Security numbers, birth dates, and other data (Tim Mullaney, "Nursing assistant faces 3 years in prison for HIPAA crime," http://www.mcknights.com/nursing-assistant-faces-3-years-in-prison-for-hipaa-crime/article/318745/ (31 October 2013)).

Risk Analyses

CEs that want to transmit PHI must conduct a risk analysis. Such an analysis consists of "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity" (HIPAA Administrative safeguards, §164.308 (a)(1)(ii)(A)). All CEs, including one-person practices, and all providers who want to receive EHR incentive payments, even those with certified EHRs, must perform such a risk analysis. An outside consultant can help, but is not required. A checklist can also help, but may not be sufficient. Moreover, a single risk analysis is not enough. A CE must continue to review, correct or modify, and update security protections over time. Risks need not be mitigated immediately. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule (http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html).

Enforcement

The HHS Office for Civil Rights (OCR) has initiated the vast majority of HIPAA enforcement ever since HITECH's 2009 enactment, resulting in imposition of civil penalties and corrective action plans (CAPs).

The settlements the government has entered into with CEs demonstrate the seriousness of HIPAA violations. In 2009, CVS Pharmacies agreed to pay $2.25 million for PHI violations. In 2012, the Alaska Department of HHS paid a $1.7 million penalty, the Massachusetts Eye and Ear Infirmary settled a fine for $1.5 million, and BlueCross BlueShield of Tennessee settled a HIPAA claim for $1.5 million. Another fine of $4.3 million was imposed on Cignet Health of Prince George's County, Maryland.

Rarely if ever do covered entities defend HIPAA charges in court. The imbalance in power between OCR and the CE is such that the defendant usually sees settlement as the best resolution. At http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/, HHS presents, in reverse chronological order, a list of recent enforcement actions resulting in settlements. Payments typically are in the 6–7-figure range. The list is not comprehensive, but it is illustrative. In 2014, for example, OCR settled with Anchorage Community Mental Health Services, New York, and Presbyterian Hospital, Concentra Health Services, and Skagit County, Washington. In 2013, OCR settled with, among others, Idaho State University, WellPoint, and Affinity Health Plan, a not-for-profit managed care plan. These agreements demonstrate that both provider and payer CEs, large and small, private and public, are at risk.

It is also instructive to consider the array of fact patterns that give rise to exposure. The commonest breaches are attributable to human error: unencrypted laptops or thumb drives left on trains or in unlocked cars, microfiches left undestroyed, misplaced paper records, or failing to follow one's organization's own policies and procedures. In the 2014 *Parkview* settlement, OCR reported that

> …Parkview took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting [a] retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician's practice. On June 4, 2009, Parkview employees, with notice that the physician was not at home, left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician's home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue. (http://www.hhs.gov/news/press/2014pres/06/20140623a.html)

Not all the breaches, however, arise from human carelessness; some are caused by deliberate misdeeds such as malware, disabled firewalls, or scam sales of x-rays (ostensibly to recover their silver).

Settlements are not limited to payments. OCR typically imposes a corrective action plan upon the CE. These vary with the circumstances, but often requires new risk analyses and risk management plans that OCR must review and approve. Usually, the CE must also report any HIPAA violations to OCR within a defined period, often 30 days.

HHS has published a list of problems that most often lead to formal investigations:

Impermissible uses and disclosures of PHI
Lack of safeguards for PHI
Lack of patients' access to their own PHI
Uses or disclosures of more than the minimum necessary PHI
Lack of administrative safeguards of electronic PHI (US Department of Health & Human Services)

HHS has also identified the CEs most frequently required to take corrective action to achieve compliance:

Private practices
General hospitals
Outpatient facilities
Health plans
Pharmacies (*id*.)

Practitioners should bear in mind that under Section 13410(e) of the HITECH Act, enforcement of the HIPAA Privacy Rule, though a federal law, is not limited to OCR. State Attorneys General are authorized to do so as well and have. See, e.g., http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=462754. OCR even provides training to state AGs for just this purpose. See http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/.

HIPAA, Privacy, and Federal Agencies

There may be no better evidence of the force and power of HIPAA than its use against federal agencies.

In November 2013, the HHS Office of Inspector General (OIG), which "fights waste, fraud and abuse in Medicare, Medicaid and more than 300 other HHS programs" (http://oig.hhs.gov/about-oig/about-us/index.asp), completed an audit of the OCR Security Rule oversight and enforcement from 2009 to 2011 (OIG, Audit (A-04-11-05025), https://oig.hhs.gov/oas/reports/region4/41105025.asp). OCR is the very office "responsible for enforcing the Privacy and Security Rules" (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/). OIG concluded that, in its oversight and enforcement of the HIPAA Security Rule, OCR did not meet all federal requirements. OIG found 39 of 60 selected records were missing one or more documents needed for security violation investigations. OCR had not "assessed the risks, established priorities, or implemented controls for its HITECH requirement to provide for periodic audits of covered entities to ensure their compliance with Security Rule requirements." OIG found that the OCR investigation files

> did not contain required documentation supporting key decisions because its staff did not consistently follow OCR investigation procedures by sufficiently reviewing investigation case documentation. OCR had not implemented sufficient controls, including supervisory review and documentation retention, to ensure investigators followed investigation policies and procedures for properly initiating, processing and closing Security Rule investigations.

OIG also found that for its information systems used to process and store investigation data, OCR had not fully complied with federal cybersecurity requirements included in the National Institute of Standards and Technology (NIST) Risk Management Framework (http://csrc.nist.gov/groups/SMA/fisma/documents/risk-management-framework-2009_bw.pdf). OIG concluded that "by not complying with Federal cybersecurity requirements, OCR increased the risk that it might not identify or mitigate system vulnerabilities." OIG noted that not following the federal cybersecurity requirements could "increase the risk of unauthorized disclosure or destruction of ePHI" in OCR's possession.

As is customary, OCR was given an opportunity to respond to OIG's recommendations. One such was: "Provide for periodic audits in accordance with HITECH to ensure Security Rule compliance at CEs." OCR stated: "While OCR agrees with the recommendation that the HITECH audit program represents an effective tool, no monies have been appropriated for OCR to maintain a permanent audit program" (OIG, "The Office for Civil Rights Did not Meet all Federal Requirements in its Oversight and Enforcement of the HIPAA Security Rule" (November 2013), https://oig.hhs.gov/oas/reports/region4/41105025.pdf). Those in private practice can relate.

Another dispute with a federal agency, though not pursued under HIPAA, illustrates the risks involved when privacy is not sufficiently protected. The ACLU claims that in response to a FOIA request, it procured a copy of a 2009 *Search Warrant Handbook* from the IRS Criminal Tax Division's Office of Chief Counsel. ACLU quotes the *Handbook* as saying "the Fourth Amendment does not protect communications held in electronic storage, such as email messages stored on a server, because internet users do not have a reasonable expectation of privacy in such communications." ACLU indicates that it also procured other evidence that the IRS has reached this conclusion (Nathan F. Wessler, "New Documents Suggest IRS Reads Emails Without a Warrant," https://www.aclu.org/blog/technology-and-liberty-national-security/new-documents-suggest-irs-reads-emails-without-warrant).

A California CE, identified merely as John Doe Company, filed a putative class action in the Superior Court of California against the IRS in March 2013, accusing 15 IRS agents of seizing 60 million medical records from 10 million patients. The complaint, available at http://www.scribd.com/doc/142305534/John-Doe-Company-et-al-vs-John-Does-1-15-IRS-Seized-60-Million-Personal-Medical-Records#scribd, alleged that the agents took, for example, psychological and gynecological counseling data and sexual/drug treatment and other medical treatment data on California state judges, members of the Screen Actors Guild, and Major League Baseball players, among many others. It claimed: "No search warrant authorized the seizure of these records; no subpoena authorized the seizure of these records; none of the 10,000,000 Americans were (*sic*) under any kind of known criminal or civil investigation and their medical records had no relevance whatsoever to the IRS search." In addition to punitive damages for constitutional violations, the complaint sought $25,000 in compensatory damages "per violation per individual."

"HIPAA-Compliant" Technologies

Purveyors of telehealth equipment or technology sometimes promote their products as "HIPAA-compliant." Many of these are highly useful. But no technology is "HIPAA-compliant." CEs and BAs are compliant, or are not. The use of technology—any technology—cannot ensure that a CE is "HIPAA-compliant." HIPAA demands more than reliance on devices or technologies with privacy-protective features or technical specifications. Certain features may indeed help a CE comply with the rules. For example, a telehealth software program may permit encryption, or the technology might require use of passwords. Such features, though valuable,

provide mere tools to help a CE comply; they do not ensure compliance and cannot substitute for an organized, thoughtful, documented set of security practices.

Text Messaging

SMS text messaging is quick, convenient, and feasible on ordinary cell phones. One need not be technically proficient to use it. Text4baby, for maternal and child health, and Text2Quit, for smoking cessation, have probably benefited tens of thousands. Historically, text messaging was risky. Such messages were unencrypted, neither party could authenticate the other, and the PHI could remain stored on the individual's device and, for unpredictable periods, on telecommunications company servers as well. The Joint Commission, originally deemed it unacceptable for "physicians or licensed independent practitioners to text orders for patients to the hospital or other healthcare setting[s]" (Standards, FAQ Details, http://www.jointcommission.org/standards_information/jcfaqdetails.aspx?StandardsFaqId=401&ProgramId=1). With improving technology, however, especially widespread use of encryption the risk is now much lower. In fact, the joint Commission recently reversed itself and now approves text messaging for transmission of physician orders. See, "Update: Texting Orders 36(5) Joint Commission Perspectives 15 (May, 2016), https://www.jointcommission.org/assets/1/6Update_Texting_Orders.pdf.

The Cloud

Using the cloud is also risky. Dropbox, for example, one of the most popular and perhaps one of the most well developed of the cloud storage providers, discusses its security and privacy features and identifies standards and regulations it complies with, at https://www.dropbox.com/help/238/en. It makes no claim, however, that it complies with HIPAA. Nor could it. Dropbox keeps metadata, including the file name, which is not secure. It also lacks the audit controls that HIPAA demands. It is possible that, with technological advances and evolution in the law, the cloud may gradually become a legally responsible place to stou PHI. At present practitioners should be leery of using the cloud for communicating about PHI.

Future

There is no reason to believe that HITECH enforcement will relent in 2016 or beyond, especially because the HITECH Act authorized the transfer of funds collected through civil monetary penalties or monetary settlements for HIPAA violations to OCR to support enforcement efforts.

HHS has published a notice of proposed rulemaking, proposing to amend the Privacy Rule to permit certain CEs to disclose the minimum necessary demographic and other information for National Instant Criminal Background Check System (NICS) reporting purposes. NICS determines whether a potential firearms purchaser is statutorily prohibited from possessing or obtaining a firearm. That category includes those who have been (1) involuntarily civilly committed; (2) found incompetent to stand trial or found not guilty by reason of insanity; or (3) otherwise determined, through a formal adjudication, to have a severe mental condition that makes the individual a danger to himself or others, or incapable of managing his own affairs. As of this writing, the final rule has not yet been published. See https://www.federalregister.gov/articles/2014/01/07/2014-00055/health-insurance-portability-and-accountability-act-hipaa-privacy-rule-and-the-national-instant.

Private Claims

Under HIPAA, there is no private right of action. That is, although a CE violating the law is vulnerable to a variety of governmental penalties, the patient whose records were compromised finds no basis in HIPAA to sue the CE. That does not mean that plaintiffs have not tried to sue over breaches of privacy or security of their private information. First, such a patient might well have an avenue of recovery under state law, independent of any asserted HIPAA violation. Second, in a handful of cases, courts have permitted state law claims supported in part by alleged HIPAA violations and pleaded as claims such as "negligence per se." Negligence lies for harms resulting from a failure to act as a reasonable person in like circumstances would act. Under negligence per se theory, a court may find a defendant who has violated a statute, ordinance, or regulation negligent as a matter of law.

On 11 December 2009, AvMed, a Florida-based health insurer, reported the theft from a locked conference room of two laptops containing unencrypted personal information on more than 1.2 million customers, including names, Social Security numbers, and other PHI. Patients brought a putative class action in Florida federal court, alleging that in failing to secure its computers or encrypt their data, AvMed violated federal health privacy rules, industry standards, and its own stated consumer protections. The Southern District of Florida dismissed plaintiffs' claims, in part because the complaint failed to allege cognizable injury. In *Resnick v. Avmed, Inc*., 693 F. 3d 1317 (11th Cir. 2012), however, the appellate court reversed the trial court's dismissal of all but two claims. It held that the plaintiffs had properly alleged an injury in fact that was fairly traceable to the theft by alleging that they had been careful with their own PHI, that they were victims of identity theft, and that their identities were stolen only after the AvMed incident. The ensuing settlement was the first to offer financial remuneration to class members who did not themselves suffer identity theft. The settlement not only provided monetary damages for customers who can show they actually experienced identity theft but also provided for

a $3 million fund from which current and former members can make claims for $10 for every year they were AvMed customers, thereby recouping the part of their premiums that plaintiffs claimed should have been used on data security. AvMed also agreed to implement data security measures consistent with HIPAA regulations, including mandatory security awareness training, new password protocols, upgrades to laptop security systems, facility security upgrades, and updates to security policies and procedures.

On 29 January 2013, a putative class action was filed in New Jersey federal court against Horizon Blue Cross for a data breach allegedly affecting 840,000 enrollees. Over a weekend, thieves stole computers cable-locked to workstations, gaining access to names, addresses, dates of birth, clinical information, and Social Security numbers. The complaint is available at http://www.garfunkelwild.com/NJHLBulletin/NJHLPDF/2014/DataBreachSpring2014.pdf. On 31 March 2015, the case was dismissed, because, said the court, an injury sufficient to confer standing was not proved. Standing refers to a party's ability to demonstrate to the court sufficient connection to and harm from the action challenged to support that party's participation in the case. Specifically, plaintiffs were unable to show that they had been or would be harmed. See Elizabeth Snell, "Data Breach Lawsuit Against Horizon BCBS Dismissed," *HealthITSecurity* (7 April 2015), http://healthitsecurity.com/news/data-breach-lawsuit-against-horizon-bcbs-dismissed.

The States

With the understandably heavy emphasis on HIPAA, state statutes are too often overlooked. Every state has some form of legislated protection of the privacy of health records, and those laws retain their vitality despite HIPAA's enactment. An exhaustive treatment of the topic would exceed the scope of this chapter, but an example or two may be illustrative.

Eleven years before HIPAA was enacted, a plaintiff successfully sued a plastic surgeon for posting patient-identifiable before-and-after photographs on TV and in a department store promotion of aesthetic surgery. Although photos could be a legitimate part of a medical record, said the court, public display without patient consent was actionable as a breach of privacy (*Vassiliades v. Garfinckel's, Brooks Bros.*, 492 A.2d 580 (D.C. App. 1985)). In a more recent case, however, the court held that violation of California's Confidentiality of Medical Information Act, Civil Code § 56-56.07, requires "more than an allegation of loss of possession by the health care provider." Rather, a plaintiff must prove that "the confidential nature of the plaintiff's medical information was breached as a result of the health care provider's negligence" (*Regents of the University of California v. Superior Court*, No. B249148, 2013 WL 5616775 (Cal. Ct. App. 15 October 2013) at *12). See also *Sutter Health et al. v. The Superior Court of Sacramento County*, C072591 (Cal. 3d App. Dist. 2014) (absent an allegation that a protected medical information thief actually viewed the stolen data, mere theft without more does not give rise to a

cause of action for nominal damages under the California Confidentiality of Medical Information Act (CMIA) (Cal. Civ. Code, § 56 *et seq*., http://www.cmanet.org/files/assets/news/2014/07/sutter-health-v-superior-court-july-21-2014.pdf)). On the other side of the country, by a statute passed unanimously in January 2015, New Jersey required health insurers to encrypt their health data. Violations entail imposition of a fine of up to $10,000 for a first offense and up to $20,000 for a subsequent offense; treble damages and a court order to pay the costs of adversely affected parties are also available. See http://www.njleg.state.nj.us/2014/Bills/S1000/562_R1.PDF. These examples illustrate the need for health professionals to understand and abide by not only federal but also state legal requirements in their practices.

Informed Consent

The standard of care for informed consent varies with the state. For a general discussion, see Paula Walter, "The Doctrine of Informed Consent: To Warn or Not to Warn," 71 *St. John's L. Rev*. 543, 545–49 (1997). Some states, such as California, have enacted specific statutes governing informed consent in telemedicine (Cal. Bus. Prof. Code § 2290.5 (2009)). Other examples include Oklahoma, which not only has developed statutory authority on informed consent but has expressly identified information that must be disclosed. See discussion of *Trow,* supra. See also 22 Tex. Admin. Code § 174.5(b).

Most states, however, have no legislation directly on point. In those states, the analysis of informed consent allegations in telemedicine cases will probably proceed along lines pertinent to informed consent generally.

The requirement to obtain informed consent derives from the unremarkable proposition that each of us is entitled to control what is to happen to his own body. Legal recognition of this principle has been black letter American law for at least a century. See *Schloendorff v. Society of New York Hospital*, 211 N.Y. 125, 105 N.E. 92 (1914). Although traditionally most closely linked to invasive procedures, in principle informed consent covers substantially everything a provider does for and with a patient, even if the body is not invaded at all.

The states follow one of three general approaches to the standard of care for obtaining consent. The approach most favorable to the provider is to require him to disclose only that information which reasonably prudent practitioners in the same field would reveal in similar circumstances. Considerably less provider-friendly is a requirement to reveal that which a reasonable person in the patient's shoes would want to know. The harshest standard, fortunately limited to only a couple of outlier states, is to demand that the professional reveal whatever this particular patient claims he wanted to know. In case of a dispute, it would not require an especially active imagination to anticipate that the patient's description of his desire for information as expressed to his clinician at the time of care, and his description of those wishes to a jury some years later, may or may not be the same.

Assuming the plaintiff patient can prove that the provider failed to divulge information obligatory under the standard of care, he must next show what the consequences were. On this question, states typically ask one of two questions: (1) what would a reasonable patient have done had she been advised of the allegedly omitted information? or (2) what would this particular patient have done had she been advised of the allegedly omitted information? This second formulation is vulnerable to the same manipulation as is the third iteration of the consent standard of care above.

In the absence of much case law to guide us, the best course for a telemental health professional to follow is to advise the client/patient that distance care may entail not only all the risks of in-person care but also those peculiar to distance care, such as power interruption. One risk to mention is that, since telehealth is still fairly new, practitioners may not even know of all the risks that patients might be exposed to.

Professional Liability

Malpractice is a form of negligence and thus a type of tort. A tort is a civil wrong. It is distinguished from a crime (an offense against the state) and a breach of contract (a failure to fulfill obligations voluntarily assumed). Professional liability in tort arises not because the practitioner committed a crime, nor because he broke his word, but because the patient was harmed because the professional failed to do as a reasonably prudent practitioner in his field would have done in similar circumstances at the time the case arose. Professional liability claims are numerous. Probably because telemedicine still has but limited market penetration, few reported cases describe claims against professionals providing this service. The plaintiffs' bar, however, is wily and persistent. Some of their number are trolling the Internet, advertising for patients, just as they do for individuals asserting asbestos claims or those hurt in auto accidents. It is naïve to imagine that distance care will be spared.

Jurisdiction

In all litigation, a fundamental issue is whether the court where the matter was brought has legal authority to entertain the claim. If it does not, it should dismiss the case for want of jurisdiction: the court lacks power to rule. The claim may be valid, but it has to be heard, if at all, somewhere else.

Historically, in malpractice litigation, jurisdiction was usually not a major issue. Doctor and patient were typically citizens of the same jurisdiction, and since malpractice cases are heard where the tort was committed, the local court typically had jurisdiction. In telehealth, of course, therapist and patient need not be in the same jurisdiction. In fact, they need not even necessarily be in the same country. Whether

a court has jurisdiction, then, depends on where, in contemplation of law, the tort was committed. In the current state of the law, when clinician and patient are not in the same jurisdiction, there is no definitive answer. The conclusion most commonly reached is that the tort occurred where the patient is, so jurisdiction lies in that jurisdiction. In some states, this principle has been established as a matter of law, e.g., 225 Ill. Stat. 60/49.5 (an out-of-state physician "providing a service … to a patient residing in Illinois through the practice of telemedicine submits himself or herself to the jurisdiction of the courts of this state." Id. at 60/49.5(e)); http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=022500600K49.5 (*Accord*, Ga. Code Ann. 43-34-31). Some have argued for the opposite conclusion, however. Since a clear answer is not yet established, it is probably best to (1) assume a case would be heard in the patient's jurisdiction and (2) comply insofar as possible with the laws of both jurisdictions.

Creating the Relationship

The first leg of the analysis needed to assess a possible malpractice claim is whether the defendant owes the plaintiff a duty. If no duty exists, there can be no breach of duty; where there is no breach, there is no case. Whether a physician–patient relationship exists is a question of law for the court (*Reynolds v. Decatur Mem'l Hosp.*, 660 N.E.2d 235, 238 (Ill. App. 1996), citing *Kirk. v. Michael Reese Hosp. & Med. Ctr.*, 513 N.E.2d 387 (Ill. 1987) but see, Mackey v. Sarroca, 35 NE 3d 631 Ill. Ct. App. 2015, (duty arises only when physician-patient relationship has been expressly established or there is a special relationship such as when one physician asks another to provide a service to the patient).

Determining whether a duty exists is ordinarily very straightforward: If X is Y's therapist, X owes Y a duty. To some extent, however, the analysis can be more complex when professional and patient are not in the same room. Physical contact between doctor and patient is not necessary to create a doctor–patient relationship (*Bovara v. St. Francis Hosp.*, 298 Ill. App. 3d 1025, 700 N.E.2d 143, 147, 233 Ill. Dec. 42 (1988) (determining which patients were angioplasty candidates)). But see *Adams v. Via Christi Reg'l Med. Ctr.*, 270 Kan. 824, 835 (2001) (no relationship arises until doctor undertakes some affirmative action). A telephone call may suffice to form a doctor–patient relationship (*Reynolds v. Decatur Mem'l Hosp., supra; Bienz v. Central Suffolk Hospital*, 163 A.D. 2d 269. 270, 557 N.Y.S.2d 139, 140 (2d Dep't 1990)). In fact, such a relationship can arise even where the physician and patient have not spoken with each other (*Kelley v. Middle Tennessee Emergency Physicians, P.C.*, 133 S.W.3d 587, 596, 2004 Tenn. LEXIS 333 (Tenn. 2004)) (whether a physician–patient relationship arose between covering cardiologist consulted by phone about a patient he never saw, nor was ever asked to see, was a question of fact for the jury).

Nonmedical advice to a patient's provider creates no professional relationship between the provider's adviser and the patient. A licensed clinical social worker

whose practice employs a life coach does not assume a provider–patient relationship with the coach's client by advising the coach to report suspected child abuse; doing so is "giving non-medical professional advice" to the coach. The same is true of a psychiatrist employed by the same practice and giving similar advice to the same coach (*Wolf v. Fauquier County Bd. of Supervisors*, 555 F.3d 311, 321, 2009 US App. LEXIS 2256 (4th Cir. 2009)).

In the current state of the law, what is needed to establish a duty in a telehealth context is thus not always clear, especially in jurisdictions that require a physical exam to create a doctor–patient relationship. In the right circumstances, a physician defendant may deny that between himself and the plaintiff, any doctor–patient relationship even existed, since prevailing on that theory would defeat the claim. In telemental health, however, such a defense will probably be more difficult to mount, because the physical separation between treater and patient is of less consequence.

The Standard of Care

Assuming a duty exists, the question then becomes whether that duty was breached. To answer, the finder of fact must determine what the standard of care is in the circumstances and whether the defendant did or did not comply therewith. The standard of care in telemedical malpractice is often said to be that which obtains in conventional, in-person care. See, e.g., Fed'n State Med. Bds., Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine (2014) (http://www.fsmb.org/pdf/FSMB_Telemedicine_Policy.pdf). In some jurisdictions, that principle is enshrined in law. See, e.g., Haw. Rev. Stat. § 453-1.3(d) (Supp. 2012). As with so many other issues in telemedical malpractice, however, few if any courts have actually addressed the issue. See *Roush v. Southern Arizona Ear, Nose & Throat*, 2CA-CV 2008-0049, Unpub. LEXIS 1167 (Ariz. App. Div. 2, 2009) (in defamation claim arising from defendant's statement that plaintiff's supposed ear problem was "all in his head," ENT providing telemedicine services to inmate was entitled to summary judgment). For an argument that, where "telemedical procedure and traditional-medical procedures are distinctive" and not, as with teleradiology, substantially identical, "the standard of care for telephysicians should be higher than the applicable standard for traditional physicians"; see Lisa Rannefeld, "The Doctor Will E-Mail You Now: Physicians' Use of Telemedicine to Treat Patients Over the Internet," 19 *J.L. & Health* 75, 100 (2004/05).

The genius of the common law is its ability to adapt to change. In most states, the standard of care is time-sensitive. One is judged by how one's peers would act under similar circumstances at the time the case arose. See, e.g., Va. Code Ann. § 8.01-581.20; N.C. Gen. Stat. 90-21.12.[2] On occasion, a failure to adopt new approaches

[2] For a discussion of pertinent case law, see Carter L. Williams, "Evidence-Based Medicine in the Law Beyond Clinical Practice Guidelines: What Effect will EBM Have on the Standard of Care?" 61 *Wash. & Lee L. Rev*. 479, 508–12 (2004).

can be a breach, even where the care complained of comports with prevailing professional practice (*Helling v. Carey*, 519 P.2d 981, 985 (Wash. 1974) (ophthalmologist held liable for failing to diagnose glaucoma in young patient even though reasonably prudent ophthalmologists did not test for it then); *Washington v. Wash. Hosp. Ctr.*, 579 A.2d 177, 180 (D.C. Cir. 1990) (hospital held liable for failing to use continuous oximetry during anesthesia); *Nowatske v. Osterloh*, 543 N.W.2d 265, 272 (Wis. 1996); *Burton v. Brooklyn Doctors Hosp.* 452 (N.Y.S.2d 875 (N.Y. App. Div. 1982)).

An issue that providers, and eventually juries, will nonetheless need to consider is whether and to what extent a professional could be held liable for failing to utilize distance care technologies. The best case for such a theory may be in telestroke. Given the impressive therapeutic benefit of consulting distant specialists via technology, now rather well recognized, it would not be surprising to see a claim brought by or on behalf of an ischemic stroke patient denied thrombolytics based on the theory that had the clinician sought a telestroke consult, a diagnosis could have been timely made and paved the way to treatment. There do not yet appear to be any plainly analogous circumstances in telemental health, but as distance care services become more widely available to emergency departments, for example, that might change. See Patricia Kuszler, "Telemedicine & Integrated Healthcare Delivery: Compounding Malpractice Liability," 25 *Am. J.L. & Med.* 297, 316 (1999) (hereinafter "Kuszler"); Angela Holder, "Failure to 'Keep Up' as Negligence," 224 *JAMA* 1461, 1462 (1973). See also Donald E. Kacman, "The Impact of Computerized Medical Literature Databases on Medical Malpractice Litigation: Time for Another *Helling v. Carey* Wake-Up Call?" 50 *Ohio St. L. J.* 617, 621 (1997).

Insurance

Given the risks inherent in all forms of healthcare and given in particular our country's obsession with litigation, clinicians need insurance coverage to avoid, or at least reduce the risk of, financial ruin. Most malpractice insurance policies, however, cover care provided by the insured within the state where he is licensed to practice only (Medical Malpractice and Liability, Telehealth Resource Centers, http://www.telehealthresourcecenter.org/toolbox-module/medical-malpractice-and-liability). Before offering distance care services, clinicians need to determine whether they are adequately protected.

Some carriers decline coverage altogether for telehealth care (S.N. Singh and R.M. Wachta, "Perspectives on Medical Outsourcing and Telemedicine: Rough Edges in a Flat World?" 358 (15) *New Engl. J. Med.* 1622, 1625 (2008); Kip Poe, "Telemedicine Liability: Texas & Other State Delve into the Uncertainties of Healthcare Delivery via Advanced Communications Technology," 20 *Rev. Litig.* 681, 698 (2001)). Besides identified risks for which there is relatively little experience on which to base underwriting judgments, there may be risks thus far not identified. Carriers may have particular difficulty in assessing risk of suit in locales

distant from the insured's. See Robert F. Pendrak and R. Peter Ericson, "Telemedicine May Spawn Long-Distance Lawsuits," *Nat'l. Underwriter*, Nov. 4, 1996, at 44. There is a possibility that litigation would entail product liability claims in addition to conventional professional negligence claims; that would tend to both complicate the litigation and increase the stakes. If, for example, a defect were alleged in a medical imaging device, its manufacturer or distributor or both could be codefendants. See, e.g., Fran O'Connell, "Telemedicine Creates New Dimensions of Risks," *Nat'l. Underwriter*, 18 September 1995, at 44; J.P. McMenamin, "Does Product Liability Litigation Threaten Picture Archiving and Communication Systems and/or Telemedicine?" 11 (1) *J. Dig. Imaging* 21–32 (1998). That risk may be relatively unlikely, however (Robert F. Pendrak and R. Peter Ericson, "Telemedicine May Soon Spawn Long-Distance Lawsuits," *National Underwriter Life & Health Financial Services Edition*, Nov. 4, 1996, at *4).

These problems do not mean that insurance is unavailable. They do suggest that for the telemental health professional, a careful, prepurchase examination of any proposed policy is in order. The best course is to obtain in writing the carrier's representation that, up to the policy limits, it will insure the provider not only for in-person care but for distance care as well.

Malpractice Claims in Telemental Health: What Lies Ahead?

> It's hard to make predictions, especially about the future.
>
> —Yogi Berra[3]

For the most part, malpractice claims in a telehealth setting will probably mirror those asserted in ordinary, in-person care. After all, telehealth is not a specialty; it is simply another way for professionals to provide their services. In most branches of medicine, we might expect to see a somewhat higher prevalence of failure-to-diagnose claims, since even with high-resolution video and peripherals, the technology does tend to limit the scope of physical examination. In mental healthcare, however, physical examination is less central to diagnosis, and so such an increase might be less likely there. Similarly, highly visual specialties, such as radiology and pathology, labor at no particular disadvantage whether examining images or microscope slides inches away or miles away. One aspect of distance care that might be relatively telehealth-specific, admittedly, is liability associated with technology failures (Kuszler, supra, 25 *Am. J.L. & Med.* at 317–18 (1999)).

The current emphasis on apologies will probably continue. See, e.g., Joe Cantlupe, "Doctors: 'I'm Sorry' Doesn't Mean 'I'm Liable'" (2011) (http://www.healthleadersmedia.com/page-1/PHY-265488/Doctors-Im-Sorry-Doesnt-Mean--Im-Liable##). The first time a plaintiffs' lawyer manages to get such an apology

[3] Spoilsport scholars actually attribute this bit of wisdom to an unknown Dane (http://quoteinvestigator.com/2013/10/20/no-predict/). Pshaw.

admitted into evidence—and that will happen in due course—growth of this phenomenon will be checked temporarily. It will resume, however, as soon as carriers recognize that the occasional disaster is offset by consistent savings.

The current push to publish practice guidelines, both in distance care and in in-person care, will probably also continue. Texas, for example, has codified guidelines into regulations. See 22 Tex. Admin. Code §§ 174.1–.12. Most states have not gone that far, but more and more organizations are publishing guidelines for use by practitioners generally and distance care practitioners specifically. In May 2013, ATA published its *Practice Guidelines for Video-Based Online Mental Health Services* (http://www.americantelemed.org/docs/default-source/standards/practice-guidelines-for-video-based-online-mental-health-services.pdf?sfvrsn=6). In July 2013, the American Psychological Association (APA) published an extensive bibliography on *Standards and Guidelines Relevant to Telemental Health*, prepared by Kenneth Drude, PhD (http://www.apadivisions.org/division-31/news-events/blog/health-care/standards-telehealth.pdf).[4] Evidence-based guidelines for clinical practice are gaining increasing legal recognition. See Agency for Healthcare Research & Quality, The National Guideline Clearinghouse (http://www.guideline.gov). For a discussion of the place of clinical guidelines in medicine, see Institute of Medicine, *Leadership by Example* (2004). The IOM has taken the position that a provider's compliance with clinical guidelines is the best indicator of quality care (Institute of Medicine, *Patient Safety: Achieving a New Standard of Care*, (2004) at 5–6).

Guidelines such as these are intended to improve the quality of care, introduce a measure of standardization, and decrease liability exposure. Though the sincerity and expertise of the developers are clear, and while there is some merit in each of these objectives, a contrarian viewpoint deserves to be aired.

First, human biology is almost infinitely variable. The wisest of graybeards, with limitless resources and the best of intentions, would have difficulty developing guidelines that could cover every clinical situation and that could be applied to all comers in all circumstances. Second, lawyers are in the word business. They are trained to scrutinize words, phrases, and sentences to spot ambiguities, inconsistencies, and weaknesses. Over time, they become proficient in these skills and can use even carefully crafted language against its author. Finally, like textbooks, guidelines can become obsolete rapidly. It takes time to assemble the author team, it takes time to debate and write the guidelines, and, even in the Internet age, it takes still more time to edit and publish them. During all that time, new discoveries are being made, new papers are being published, and new approaches to management of clinical problems are getting developed. The guideline writers are necessarily shooting at a moving target.

[4] In April 2012, the American Psychiatric Association recommended that the VA's Office of Mental Health Services (OMHS) "work more closely with VA's Office of Rural Health (ORH) on best practices in meeting the mental health needs of rural veterans and in hiring and retaining rural psychiatrists and expanding telepsychiatry."

In an effort, perhaps, to cope with clinical complexity, multiple guidelines may be available for a given condition or procedure. See Lori Rinella, "The Use of Medical Practice Guidelines in Medical Malpractice Litigation – Should Practice Guidelines Define the Standard of Care?" 64 *UMKC L. Rev*. 337, 353 (1995); Troyen Brennen, "Practice Guidelines and Malpractice Litigation: Collision or Cohesion?" 16 *J. Health Polit. Policy Law* 67–85 (1991). The effort to accommodate the variations inherent in human biology tends to diminish the ability of guidelines to create bright-line tests of compliance or noncompliance with the standard of care. Moreover, for some guidelines, there is little or no scientific foundation (Rinella at 354). It would be ironic indeed if, in this *Daubert*[5] era, advocates for the health professions or for tort reform more generally relied upon guidelines tending to defeat the courts' relatively new and highly welcome effort to police the effort to pass off junk science for the genuine article.

There is good reason to doubt that practice parameters will diminish the prevalence of substandard care and defensive medicine (D. Garnick, A. Hendricks, and T. Brelinan, "Can Practice Guidelines Reduce the Number and Costs of Malpractice Claims?" 266 *JAMA* 2856 (1991)). Guidelines cannot replace medical judgment; hence, they may provide a feeble defense. And, of course, plaintiffs may be able to use them to advantage. See Michelle M. Mello, "Of Swords and Shields: The Role of Clinical Practice Guidelines in Medical Malpractice Litigation," 149 *U. Pa. L. Rev*. 645 (2001) (arguing against the use of guidelines because, inter alia, they are not in fact generally followed in actual practice). To the extent guidelines are drafted to control costs of care, for example (see, e.g., C. Havinghurst, "Practice Guideline for Medical Care: The Policy Rationale," 34 *St. Louis Univ. L. Rev*. 777 (1990)), plaintiffs will attack their use and, more importantly, will sing the familiar strains of their favorite hymn (*Profits Over People*). Moreover, the finder of fact typically remains at liberty to consider other evidence and to reject practice parameters as establishing the standard of care (Edward Hirshfeld, "Should Practice Parameters be the Standard of Care in Malpractice Litigation?" 266 *JAMA* 2886 (1991) (arguing against national implementation of guidelines to set the standard of care)).

The faith that guidelines will provide the shield needed to protect providers from the slings and arrows of outrageous lawsuits may be misplaced. According to Hyams et al., "Practice guidelines and malpractice litigation: A 2-way street," 122 *Ann. Int. Med*. 450–55 (1995), clinical practice guidelines are used in an inculpatory fashion twice as often as they are used to exculpate (54 % v. 23 %). See also Mehlman, M.J., "Medical Practice Guidelines as Malpractice Safe Harbors: Illusion or Deceit?" 40 *J.L. Med. & Ethics* 286 (2012). When guidelines are used to exonerate the defendant provider, however, the evidentiary value was usually sufficient for dismissal.

Hence, guidelines ought not be rejected out of hand. But they need to be developed with the clear understanding that the adversaries of healthcare professionals will attempt to use them not as shields but as swords. At times, they will succeed.

[5] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993), a case restricting what expert testimony will be accepted into evidence in federal and some state courts.

Clinicians should not assume that good faith efforts to comply, nor even slavish adherence to the very best of guidelines, will prevent claims, or even successful claims.

Reimbursement

Reimbursement for distance care remains limited. The government fears overutilization and so has imposed severe restrictions on its reimbursement for telehealth of all kinds. Historically, private carriers have generally followed in the footsteps of CMS, but in recent years increasing number of commercial carriers have begun offering coverage when Medicare does not.

There has been considerable, if gradual, liberalization of reimbursement rules, and that is likely to continue and probably to accelerate. First, although telemedicine was not initiated to further the ACA goal of expanded emphasis on outpatient care, it is nonetheless beautifully designed for that purpose. If we are serious about saving costs by decreasing our reliance on inpatient management, and institutionalized care, then we will need to provide enhanced communication between providers and patients. In a lot of ways, telemedicine is simply a communications mechanism. Second, popular demand will require expansion of telemedical services. We use the Internet to chat, buy and read books, secure hotel and travel reservations, watch movies, order dinner, and purchase medications, among numerous other functions. We will demand healthcare services in the same way, and Medicare will eventually pay for it. Third, reimbursement is apt to increase as we continue to wander farther from fee-for-service care.

In certain circumstances, Medicare does pay for telemental health services now. The patient must reside in a designated rural health professional shortage area or in a county outside of a metropolitan statistical area. Except in federal pilot programs in Hawaii and Alaska, the patient must be located at a healthcare facility, such as a community mental health center, and engage in real-time, interactive communication with his provider. Under current law, distance care of a patient at home generally cannot be reimbursed. Nor is store-and-forward technology a covered service. The practitioner, however, is eligible for reimbursement irrespective of his location. Not every type of provider is eligible for reimbursement, though most are, including psychologists (42 C.F.R. §410.78).

Several new developments have expanded the opportunities for Medicare reimbursement: a modification of "regulations describing eligible telehealth originating sites to include health professional shortage areas (HPSAs) located in rural census tracts of metropolitan statistical areas" and the addition of two new codes. Codes 99495 and 99496 are used to report transitional care management (TCM) services. Code 99490 is used to report care coordination services, and all of these, subject to various limitations, can be reimbursed when provided at a distance. For a description of Medicare's approach, see http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/Downloads/MM8553.pdf.

The commentary sheds some additional light on the meanings of these Codes:

- CPT Code 99495
  - Transitional care management services with the following required elements: Communication (direct contact, telephone, electronic) with the patient and/or caregiver within 2 business days of discharge
  - Medical decision making of at least moderate complexity during the service period
  - A face-to-face visit, within 14 calendar days of discharge
- CPT Code 99496
  - Transitional care management services with the following required elements: Communication (direct contact, telephone, electronic) with the patient and/or caregiver within 2 business days of discharge
  - Medical decision making of high complexity during the service period
  - A face-to-face visit, within 7 calendar days of discharge

Transitional care management, then, means one in-person visit within a specified period post-discharge, in combination with services not in person that may be performed by the physician or other qualified healthcare professional and/or licensed clinical staff under his direction.

In 2013, CMS modified the definition of "rural" under Section 332(a)(1)(A) of the Public Health Service Act (PHSA). Originally, CMS interpreted "rural" under Section 1834(m)(4)(C)(i)(I) of the PHSA to mean "an area that is not located within a metropolitan statistical area (MSA)." Its final rule modified the definition of "rural" to include "geographic areas located in rural census tracts within MSAs." As ATA puts it, the government is thus beginning to pay for telehealth at "the fringes of metropolitan areas." CMS is also adding coverage (CPT codes 99495 and 99496) for patient–physician communications in transitional care management and chronic care and is slightly increasing telehealth reimbursement for physicians from $24.43 to $24.63, up from $20 in 2011. "Transitional care management services" can be reimbursed for those "whose medical and/or psychosocial problems require moderate or high complexity medical decision making during transitions in care from an inpatient hospital setting (including acute hospital, rehabilitation hospital, long-term acute care hospital), partial hospitalization, observation status in a hospital, or skilled nursing facility/nursing facility, to the patient's community setting (home, domiciliary, rest home, or assisted living)."

The emphasis on rural care creates a need to determine what geographic regions qualify. Population growth and demographic shifts can render any given determination obsolete. Providers need to check demographic data periodically. CMS is developing an online rural HPSA analyzer and will announce its availability on the CMS Medicare telehealth web page. See http://www.ers.usda.gov/data-products/rural-urban-commuting-area-codes.aspx#.UdxUEUHVDw9. To avoid mid-year interruptions, CMS will make the determinations on 31 December of the prior year.

On Jan. 1, 2015, the Medicare program began making payments under CPT code 99490 for management and care coordination services provided virtually rather than in-person. Under the rule, providers managing patients with chronic illness may delegate part of the work to nurses. CMS will allow providers to count the time they spend reviewing data towards the 20-minute monthly minimum time required to bill the chronic care management code. Reimbursement is available for service rendered to patients in their homes, a first under the program On April 11, 2016. CMS announced its comprehensive Primary Care Plus (CPC+) model, expanding opportunities for reimbursement through a policy that more nearly approximates capitations. As is true with the chronic care management scheme, CPC+ imposes new and significant burdens on providers, but provides an opportunity to expand distance care service. The probability is good that further liberalization of coverage and payment will gradually increase over time.

Another advance toward broader reimbursement is found in the 2014 National Defense Authorization Act (https://www.govtrack.us/congress/bills/113/hr1960/text). Under section 704, service members transitioning to civilian life are eligible to receive 180 days of health insurance coverage for services provided through telehealth.

The Mental Health Parity and Addiction Equity Act, Pub.L. 110–343, 122 Stat. 376, is also pertinent here. Although not specific to distance care, the Departments of HHS, Labor, and Treasury jointly issued a final rule implementing the Paul Wellstone and Pete Domenici Mental Health Parity and Addiction Equity Act (MHPAEA) in November 2013. See https://www.federalregister.gov/articles/2013/11/13/2013-27086/final-rules-under-the-paul-wellstone-and-pete-domenici-mental-health-parity-and-addiction-equity-act. The MHPAEA prohibits group health plans and health insurers from imposing financial requirements such as co-pays, deductibles, and treatment limitations applicable to mental health and substance use disorder benefits that are more restrictive than the limitations applied to medical and surgical benefits.

State Approaches to Reimbursement

At least 48 state Medicaid programs, and the District of Columbia reimburse in some form for telemedicine, though no two state laws are alike and reimbursement policies vary considerably, because each state sets its own. Center for Connected Health Policy, "Telehealth Medicaid and State Policy (2015), cchpca.org. The only states that at this writing *do not* cover telemedicine under Medicaid are Connecticut and Rhode Island. AJA," State Telemedicine Gaps Analysis: Coverage and Reimbursement (May, 2015).

Effective 1 October 2013, Texas Medicaid approved procedure code 99090 for deploying vital sign monitors into the home for a reimbursement of $50. Using this code with modifier GQ yields $9.45 a day for patient monitoring. Physicians also receive new reimbursement under code 99444. This new code pays $57.20, to

review the patient's vitals once every 7 days. None of this is directly relevant to reimbursement for telemental health services. It may presage, however, a new willingness to acknowledge the value of distance care. If so, reimbursement may become more widely available in future.

A development in recent years that continues to show signs of vitality is the movement toward telehealth parity. As of this writing, some 29 states have enacted legislation providing that, when a carrier reimburses for a service done in-person, it must also reimburse when that same service is provided remotely. See Brian Dolan, "Delaware's telehealth parity bill becomes law as Congress re-floats nationwide version," *MobiHealth News* (8 July 2015), http://mobihealthnews.com/45124/delawares-telehealth-parity-bill-becomes-law-as-congress-re-floats-nationwide--version/. These states include Arizona (partial), California, Colorado (partial), Delaware, the District of Columbia, Georgia, Hawaii, Indiana, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nevada, New Mexico, New Hampshire, New Mexico, New York, Oklahoma, Oregon, Tennessee, Texas, Vermont, and Virginia.

The likelihood seems good that, over time, both public and private reimbursement for telehealth services will grow more generous. At the same time, the cost of connectivity may well fall. Once the financial barriers are lowered, or perhaps overcome entirely, the benefits of distance care will become both more widespread and more obvious.

http://www.springer.com/978-3-319-23735-0

Career Paths in Telemental Health

Maheu, M.M.; Drude, K.P.; Wright, S.D. (Eds.)

2017, XXXI, 309 p. 2 illus. in color., Hardcover
ISBN: 978-3-319-23735-0