Available online at www.sciencedirect.com

ScienceDirect

Cognitive and Behavioral Practice 22 (2015) 258-268

Cognitive and Behavioral Practice

www.elsevier.com/locate/cabp

Legal, Regulatory, and Risk Management Issues in the Use of Technology to Deliver Mental Health Care

Greg M. Kramer, Julie T. Kinn, and Matt C. Mishkind, *National Center for Telehealth and Technology*

Improved telecommunications networks and technologies have resulted in increased availability of technology-delivered mental health services to patients anywhere at any time, in particular to those patients in rural and isolated communities. This increased use of technology to deliver mental health care over a distance raises a number of regulatory issues relevant for safe and effective practice. In this article we cover some of the key legal, regulatory, and risk management issues in today's telemental health (TMH) environment, with specific emphasis on licensure, malpractice, credentialing and privileging, security and privacy, and emergency management. The article further discusses some risk management considerations related to mobile health applications and the use of social networking to deliver TMH services. The information presented is expected to alleviate some risk concerns and provide a framework to effectively manage risk associated with telemental health care. This information should give any new or seasoned telemental health provider the foundation necessary to effectively manage risk associated with telemental health care.

The information age is an exciting time to deliver mental health care as advances in telecommunications technologies have made it increasingly possible to deliver a range of safe and effective services that reach beyond the confines of traditional clinical settings. This substantial expansion of technologies over the past two decades has further prompted a reconceptualization of human-technology interactions within the health care industry. The use of technologies presents the health care industry with opportunities to economize and streamline a greater proportion of care to the patients who need it most (Steinhubl, Muse, & Topol, 2013). Private practitioners, hospitals, and public service stakeholders have recognized that as all generations continue to increase their use of and comfort with technology, the environments where mental health care can occur will continue to expand. The U.S. Department of Veteran Affairs, for example, has an established telehealth program and is planning to continue to increase its use as a way to meet the growing demand for patient-centric health care delivery services (see, e.g., Darkins, Foster, Anderson, Goldschmidt, & Selvin, 2013; Petzel, 2013). The Department of Defense, likewise, has telehealth programs in all branches of services, and even uses telehealth in operational and other deployed settings (Poropatich, Lai, McVeigh, & Bashshur, 2013).

The commonly used terms telehealth (TH) and telemedicine have many definitions, but they broadly refer to methods of delivering health care via technology over a distance. Telemental health (TMH; sometimes referred to as telebehavioral health) refers to a subset of TH that uses telecommunications technologies and related communication networks to provide psychological, psychiatric, traumatic brain injury, and other mental health and substance use care services from a distance. Similar to the more broadly defined telehealth, TMH "is not a clinical service itself, but rather a mode of service used to connect patients or providers located in one location with providers in a distant location" (Kramer, Ayers, Mishkind, & Norem, 2011).

A growing body of literature has demonstrated the benefits and effectiveness of delivering mental health care using technology such as video-teleconferencing (Backhaus et al., 2012; Grady et al., 2011; Hilty et al., 2013; Richardson, Frueh, Grubaugh, Egede, & Elhai, 2009). Given the established benefits of TMH, it is important that those engaged in its practice remain aware of current rules, guidelines, and regulations governing the provision of services from a distance. While these legal and regulatory issues may be seen as barriers by some, the increasing use of TMH throughout the United States and other countries demonstrates that there are few absolute barriers to providing safe and effective TMH services, and many other so-called obstacles to using TMH have been reduced (Brooks, Turvey, & Augusterfer, 2013).

This article is intended to provide an overview of some regulations and standards in place that make TMH not only an effective mode of health care delivery but also a safe one. The good news is that there are effective risk-management strategies to provide safe, effective,

Keywords: Telemental health; Mobile health; Safety; Policy; Regulations

high-quality services while abiding by legal and regulatory controls. Our goal is to make one thing clear to health services personnel at any stage in their career: *Using technology to provide mental health care is achievable and becoming easier all the time.* To meet this goal, the content of this article is divided into three main sections. Section 1 focuses on notable regulations governing the safe and effective provision of TMH services via synchronous (live, two-way interactive audio/visual) technologies such as video teleconferencing (VTC). These regulations include health care licensure, malpractice liability, and credentialing and privileging. Section 1 concludes with an overview of some standard risk-management practices to include those for nontraditional settings such as a patient's home. Section 2 focuses on mobile health (mHealth) applications (apps) and best practices for providing TMH services using mobile devices. Though synchronous communication (live, real-time, two-way interactive) is generally the most common form of TMH care delivery, there is ongoing research into asynchronous (communication happening at different times) forms of TMH care (Odor et al., 2011; Yellowlees, Odor, Parish, Iosif, Haught and Hilty, 2010; Yellowlees, Shore and Roberts, 2010), and mobile health is one way to provide this type of care. Section 3 focuses on the use of social media to provide TMH services. Although social media regulations are in their infancy, TMH stakeholders should be aware of considerations to using this media to provide services.

This article does not provide an exhaustive review of all regulations and standards governing the range of TMH services. For example, we do not attempt to address any of the issues or regulatory concerns that may specifically apply to psychotherapy conducted online without using video technology. We have selected to focus on these three sections as we believe they cover the majority of considerations while providing a good foundation for anyone interested in engaging in most forms of TMH services. It should be noted that this article is not intended as a legal review, but rather an overview of the TMH regulatory environment. When in doubt, we encourage all TMH professionals to obtain local legal opinion.

Regulatory Issues Governing Synchronous Telemental Health Services

Health Care Licensure

One of the great promises and selling points of TMH has been its potential to address the unmet health care needs of those living in rural or remote areas and other underserved populations. A 1998 American Psychiatric Association (APA) report spoke of that promise: "[O]riginally conceived to enhance access to health care for the geographically hard-to-reach and the underserved . . . telemedicine is much broader and will become the way we are all served—whether underserved or not—with greater efficiency, continuity, and timeliness" (American Psychiatric Association, 1998). One of the barriers to this vision, however, has been the regulatory environment defining how and when TMH providers can cross over jurisdictional boundaries—for example, state lines—to provide care. Consequently, compliance with appropriate laws regarding health care licensure is one of the most immediate concerns raised prior to engaging in TMH practice. Although additional reform is required, there are recent and continuing developments to reduce licensure concerns across jurisdictional boundaries.

Legal Background in the United States

In the United States, the individual states, and not the federal government, have historically had control over establishing and enforcing licensure requirements for a wide range of health care professionals, including mental health professionals (U.S. Department of Health and Human Services, 2010). State authority to do this is generally considered a "police power" that comes from the 10th Amendment of the U.S. Constitution. Inherent in this "police power" is a priority to protect the health, safety, and welfare of citizens within their borders (U.S. Department of Health and Human Services, 2010). Since state licensing boards are primarily focused on protecting the public services received within their state, they view the delivery of health care services as occurring where the patient is located. Along with that is the historical expectation that the health care professional providing services is licensed and located in that same state, so if harm occurs the state can intervene to protect its citizens. As a result, one of the most discussed challenges that telehealth may present regarding licensure is how individual states can continue to protect their citizens for care provided within their state when the professional providing the care is physically located in another state. The general solution has been to require a provider to maintain a license where the patient is located.

Prior to the expansion of available telehealth services, questions related to practicing health care across state lines, and thus maintaining multiple licenses, rarely arose because diagnosis and treatment almost exclusively occurred face-to-face, and within one state (Ameringer, 2011). The expanded use of some telecommunications technologies, however, has expanded the use case scenarios such that providers and patients can connect virtually anywhere in the world. While many health care professionals may want to expand their practice into several geographies, the process of obtaining multiple licenses is often a financial and administrative burden (Miller et al., 2005). With the emergence and increased use of TH, commentary on the limits of a state-based licensure system and debates on potential solutions have increased (Ameringer; Gupta & Soa, 2010; Miller et al.).

Some proposed solutions include allowing states to create interstate licensure compacts with each other whereby states can mutually recognize the licenses of other participating states (in general or for specific purposes), creating a special TH license, and creating a national license (Ameringer; Gupta & Soa).

The call for TH licensing reform has prompted various national health regulation authorities to consider alternative strategies to address the issue. The Federation of State Medical Boards, the Association of State and Provincial Psychology Boards, and The National Council of State Boards of Nursing have all undertaken efforts to address licensure portability for health care professionals in different ways (see organizational websites and Kramer, Mishkind, Luxton, & Shore, 2012, for fuller discussion of efforts of each to date). Further, the American Telemedicine Association recently launched a website called www.fixlicensure.org that is dedicated to reforming the state-based medical licensing system in favor of a national license portability system. Unfortunately, there remains no consensus on how to address portability of licensure for health care professionals, at least within the United States, with different professional organizations advocating for different solutions.

Sample Success Story

Although no single TH licensure solution has gained universal support, expansion of licensure portability and the ability to practice across state lines has occurred at the federal level. For some time, certain federal government agencies (e.g., Department of Defense, Veteran Affairs, and Indian Health Services) have followed policies based on statute and/or case law that allow some categories of their respective health care practitioners licensed in any state to practice their federal duties in all states. Within the Department of Defense (DoD), this preemption over individual state licensure requirements previously allowed "members of the Armed Forces" to perform their authorized health care duties in any state, as long as the individual was licensed to practice in one state (Title 10, United States Code, Section 1094(d)). That statue was recently amended to expand the categories of DoD TH providers granted portability of licensure to include civilian employees of the DoD, personal services contractors, and select others when performing their federal duties (Title 10, United States Code, Section 1094(d), as amended by Section 713 of the National Defense Authorization Act for Fiscal Year 2012). This legislative change was seen by many as a positive step towards establishing a precedent for expanding the use of TH, and several additional legislative proposals have been submitted to expand licensure portability to additional classes of federal employees and to other federal organizations.

Ongoing Challenges at the State Level

While licensure developments at the federal level are promising, they do not currently impact all federal employees, nor do they impact private sector clinicians. For the nonfederal TMH clinicians, cross-state licensure remains a challenge without a widely accepted solution, and those that do wish to practice across state lines need to understand how to safely provide care under the current state-based licensure system, including the probability of obtaining multiple state licenses to practice clinical TMH services. While it is believed that the vast majority of TMH encounters are conducted safely and within the scope of existing regulations, case examples of unsafe practices do exist. In one case, a psychiatrist licensed to practice medicine in Colorado was sentenced to 9 months in county jail because he had prescribed fluoxetine to a California resident whom he did not examine in person (rather, he administered an on-line questionnaire; *Hageseth v. Superior Court*, 2007). The physician was convicted of practicing medicine without a license after the patient obtained the prescription and died by suicide. Although the actual conviction was for practicing medicine without a license, many aspects of this case focused on other relevant issues, such as online prescribing and whether it is an appropriate standard of care to prescribe medication without actually physically examining a patient. A full discussion of online prescribing and the Ryan Haight Act (H.R. 6353, 2008) that regulates Internet prescribing is beyond the scope of this article. Appropriate telemedicine standards of care are evolving, but valid concerns remain regarding acceptable practices, particularly in the area of tele-prescribing. Physicians who wish to practice and prescribe medication via electronic means should become familiar with this act and with state medical practice law (see Natoli, 2011, for a discussion of two key issues related to telemedicine and prescribing: the physical examination requirement and the preexisting physician-patient requirement). It is also recommended that physicians who are seeing potential telemedicine patients for the first time review applicable laws, regulations, and the literature to ensure that their initial examination does not fall below standard medical care and/or violate local law.

The good news is that many states are developing, reviewing, and modifying TH licensure requirements and other aspects related to TH practice. These laws and regulations vary in terms of specific licensure and practice issues they address, with some merely defining TH, some providing guidance on informed consent and information management and assurance issues related to TH, and some defining acceptable TH services one can provide in a state without a full license. Unfortunately, there is no uniformity in how state TH laws address licensure requirements and how they define whether and to what extent someone may

practice TH within their state, with some laws general to all health care providers, some specific to certain health professions, and others silent on the full range of professionals they may apply to. For example, according to one article, only 3 of the 22 states that had TH laws at the time of publication applied specifically to psychologists (although interpretation may generalize): "laws in the additional 19 states with telehealth laws do not appear to apply to psychologists at this time" (American Psychological Association Practice Organization, 2010). This could have a different impact for a social worker as opposed to a psychologist. Some state health practice statutes allow mental health professionals to obtain a temporary license to practice within their state for a maximum number of days per year under certain conditions. Provisions such as this may provide some opportunity for a TMH clinician who wishes to simply contact patients on a limited basis, when either the clinician or the patient is out of state due to work, education, or vacation. Some state statutes also speak to the technologies/type of services covered while others do not define the types of services covered with any specificity, and may have different applicability depending on individual circumstances.

Resources are available to help identify new initiatives and advances in licensure requirements. There are reviews of the current state TH laws available (American Psychological Association, 2010) and a way to track ongoing state TH legislation (ATA 2013 State Telemedicine Legislation Tracking). The above information is not intended to dissuade someone from practicing across state lines. On the contrary, we hope that by highlighting the noted resources and considerations we have provided the knowledge set to initiate a well-conceived expansion of TMH services.

Malpractice Liability

While licensure is often the initial concern raised by practitioners new to TMH, malpractice liability is an equal or possibly even greater issue to consider. Similar to the licensure example above, most cases of "tele-malpractice" to date have occurred when a physician has issued a prescription over the telephone or Internet without first examining the individual in person (Natoli, 2009). However, as the range of technologies used to deliver care (e.g., video-teleconferencing, Internet, mobile phone) and the settings where TMH care is delivered (e.g., patient homes) increases, it is likely that malpractice issues related to mental health practice using technology will also increase. This section will address the main malpractice issues that *could* occur with TMH practice.

In the United States, individual states have the authority to regulate malpractice insurance within their borders. And, as is the case with licensure laws, states vary widely in their insurance requirements and regulations (Gupta & Soa, 2010), with the main similarity among state insurance laws being that a health care professional have some form of malpractice insurance if providing care in his/her state. The lack of standard state-based regulations and requirements is compounded by malpractice liability insurance policies that were developed long ago to cover traditional in-person encounters. As a result, many of the insurance companies have not fully considered the issue of tele-practice, nor have they considered the issue of providing care across state lines.

In the typical medical malpractice case, liability issues are rather straightforward as the alleged "injury" occurs in the state where the treatment occurred and the patient–provider relationship is established when the patient and provider first meet for a face-to-face visit. TMH practice raises additional questions about when and how a patient-provider relationship is established due to the different ways that initial contact may occur. For example, does an initial phone consultation, an email, or even a brief live Internet connection establish professional contact and a relationship? Although there are no general legal answers, it seems reasonable to assume that a professional relationship can be established through any medium. In light of this, one risk management recommendation is to assume that any mental health service a patient may reasonably rely upon as professional advice could establish a professional relationship (Chee, 2010). And finally, in thinking about what might constitute an appropriate standard of care in TMH, it is safe to assume that TMH health providers have a similar duty of care to patients as when providing face-to-face care (Natoli, 2009), though some states may have additional regulations (e.g., informed consent), and many states require a physician to establish a bona fide relationship with the patient (usually via in-person exam) before prescribing.

Licensure and Malpractice Liability Risk Management Recommendations

Licensure and malpractice liability requirements and regulations present several questions, many without clear regulatory answers. But as is evidenced by the tremendous growth in effective and safe TMH care nationwide, these issues should not be viewed as absolute barriers. In part, this is due to the continued standardization of reasonable risk management strategies, even when no clear answers are available. Below are some *general licensure and malpractice liability risk management considerations* to promote safe and effective TMH services.

1. The best way to ease any licensure concerns is to obtain a professional license in any state that one wishes to practice. While many clinicians currently

do this and consider the financial and administrative burdens to be the cost of doing business (and often make up for the cost with the expansion of services), others are unable to justify the resources necessary to maintain multiple licenses. Consider what services you may want to provide, and before making a decision, investigate the current laws that may exist in any state you wish to practice to understand the legal nuances in state law that applies most directly to *you and your situation*. Contact the applicable state professional board within any state that you wish to practice *before* providing services in that state to confirm whether the board has any written policies on what constitutes legal and ethical TMH practice within that state (American Psychological Association Practice Organization, 2010). State health practice statutes may contain information on what is and what is not authorized practice in an individual state and may contain information relevant to malpractice liability.

2. As with licensure, there is always the option of obtaining additional malpractice liability coverage for practice in another state. A recommended first step, however, is to look into one's current malpractice liability insurance and see if it covers tele-care or provides coverage for care provided to a patient physically located in a state different from where the provider is located (some may cover practice in any state where the clinician is licensed). If there are any questions, concerns, or omissions, do not hesitate to contact the malpractice insurance carrier and, when possible, obtain written clarification on these issues from your insurer. Keep in mind that many of these issues are unresolved and many traditional insurance carriers may not have or easily divulge sufficient answers. For example, one informal survey of professional liability insurance companies attempted to obtain information by phone about their telepsychiatry policies and found the general answer was that such requests are handled on a case-by-case basis and that there was no standard approach (Hyler & Gangure, 2004). Based on this, it is recommended that you are assertive in attempting to get answers and document any verbal conversations. And the more people that ask, the more likely insurance carriers are to develop standard telehealth policies.
3. Assume that any contact with a patient or potential patient using any form of technology (email, phone, Internet chat), however brief, may create or be considered part of a professional relationship, particularly if it is reasonable to believe that the patient may rely upon that contact as professional advice.
4. Stay current on TMH research, guidelines, standards, and policy and regulation changes. The TMH Special Interest Group of the American Telemedicine Association has published three best practices resources (Grady et al., 2011; Turvey et al., 2013; Yellowlees, Shore, & Roberts, 2010), and published guidelines exist that focus on children and adolescents (Myers & Cain, 2008). Other professional mental health organizations such as the American Psychiatric Association, the American Psychological Association, and the National Association of Social Workers have also produced some information on TMH (see and search their respective websites for information). Also, there are federal organizations (DoD TMH Guidebook by Kramer et al., 2011) and state professional organizations (Ohio Psychological Association, 2009) that have created TMH information.
5. Finally, consider becoming involved in or establish a local community of TMH providers for ongoing consultation. Local peers in the community often offer a great source of information and reassurance on best practices within the local community. Anyone wishing to practice in another state is encouraged to seek out others in that state that may already have the answers you seek. A local attorney may also have relevant helpful information in terms of understanding how the presence or absence of specific regulations may apply.

Credentialing and Privileging

Credentialing and privileging (C&P) is another regulatory issue that has specific impact on the ability to deliver TMH services, especially within hospital settings. Hospitals owe a duty of care to their patients (Fleisher & Dechene, 2004), and one way to ensure this duty is by limiting the privilege to practice to those with the appropriate and verified credentials. The C&P process thus has two general parts: credentialing (the "C") is the procedure for evaluating and verifying individual qualifications (e.g., diploma, license), while privileging (the "P") is the process of evaluating those qualifications in order to determine that individuals are competent to provide care within their appropriate medical specialty (e.g., psychiatry, dermatology). The C&P process typically requires that the health care provider produce and present documentation, and the hospital verify and review the documents and then decide whether to grant certain privileges to practice within the hospital. While there are general standards for required documentation and the overall process, a great deal of variability can exist given the requirement of hospitals to maintain local administrative processes.

The Centers for Medicare and Medicaid Services (CMS) issues standards for certifying hospitals, including requirements for credentialing and privileging health care providers. Until recently, regulations required TH

providers to obtain local privileges at each hospital site where they wished to see patients. The process variability and need to maintain privileges at more than one hospital have traditionally been burdensome for TH providers and, to some extent, the hospital administrative staff responsible for revalidating credentials every few years. After much public comment on the issue, CMS released a new regulation on telemedicine credentialing and privileging in 2011 (42 Code of Federal Regulations, Part 482 and 485). The new rule streamlines the TH credentialing and privileging process by allowing the originating site hospital to rely upon the credentialing and privileging decision of the distant site facility (known as "privilege by proxy") if certain conditions are met. Those conditions include: (a) the distant site (provider) hospital is a Medicare-participating hospital; (b) there is a written agreement in place to do this between the sites; (c) the distant site practitioner is privileged at the distant site hospital, with the distant site hospital having a list of privileges; (d) the distant site practitioner holds a license issued or recognized by the state that is receiving the telemedicine services; and (e) the originating site hospital must have evidence of internal review of the distant site practitioner's performance, including any adverse events and complaints (42 Code of Federal Regulations, Part 482 and 485). While the new rules are specific to telemedicine, they have a broad definition of telemedicine ("overall delivery of healthcare") (42 Code of Federal Regulations, Part 482 and 485) that likely includes TMH services.

The Joint Commission (TJC) followed suit and issued telemedicine standards similar to CMS (Joint Commission Perspectives, 2012, Standard MS.13.01.01 and Standard LD.04.03.09). Other accrediting organizations, such as the Accreditation Association for Ambulatory Health Care, Inc. (AAAHC), have also issued written guidance that the CMS TH regulations for "privileging by proxy" are allowable (F. Chapman, personal communication, May 22, 2012), though AAAHC has not yet issued specific standards on TH services. The development of new TH standards for credentialing and privileging is one area where the TMH field may see immediate regulatory improvements, though how exactly individual hospitals and large health care organizations will use this regulation to improve the C&P process is still to be determined. The more that hospital administrators and individual clinicians engage in this new regulation, the more likely hospitals will be to work on creating more supportive C&P processes.

Clinical Practice to Manage Risk

The legal and regulatory challenges described above represent some of the overarching barriers facing TMH practitioners. In addition to the risk management strategies discussed throughout this article, there are also some clinical practice considerations that can help manage risk when using technology to provide mental health care. We mention a few of these below.

Informed Consent

Informed consent is generally considered a necessary and ethical standard of care for mental health. Likewise, since TMH is a method of delivering mental health services and not a different service per se, there is no reason to believe that requirements for TMH informed consent are any less than they are for traditional in-person mental health encounters. Thus, in the absence of any explicit regulatory guidance, it is safe to assume that informed consent prior to an initial TMH health encounter is a standard of care. It is recommended that this informed consent occur with the patient in real time and that all laws regarding the form of the consent (verbal or written) are followed (Turvey et al., 2013). Even if verbal consent is sufficient, it is always good practice to document in writing that informed consent occurred and to what elements were consented. It is important to know that several states have specific statutory requirements for what constitutes valid TH informed consent, so TMH clinicians should review any applicable regulations in their state, as those statutes may contain specific consent elements (American Psychological Association Practice Organization, 2010). In the absence of specific guidance on what constitutes valid informed consent, there are some recommended TMH informed consent elements, including: confidentiality and limits to confidentiality when using electronic communications; emergency plan; process for documentation and storage of information; potential for technical failure and procedures for coordination of care with other professionals; protocol for contact between sessions; and conditions under which TMH services are terminated and a referral for face-to-face care made (Turvey et al.).

Security and Privacy Considerations

Patient privacy, confidentiality, and security often raise concerns for TMH practitioners (see Hyler & Gangure, 2004, for specific definitions of these terms within the context of telepsychiatry). Compliance with the Health Insurance Portability & Accountability Act of 1996 (HIPAA) is the foremost issue to address when discussing protection of health data since the use of technology to deliver mental health care introduces new forms of patient data transmission (e.g., VTC, Internet, mobile phone apps). Be aware that as a result of new HIPAA rules enacted in 2013 as part of implementing the Health Information Technology for Economic Clinical Health (HITECH) Act, the fines and consequences for HIPAA noncompliance are even greater (78 FR 5565, 2013). The American Medical Association has

written a summary of the new rule (http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf) and others have summarized HIPAA and the issues related to VTC and mobile health data security (Kramer et al., 2012; Luxton, Kayl, & Mishkind, 2012; Turvey et al., 2013; and Yellowlees, Shore, et al., 2010). Based in part on all the available information and guidelines, we offer a few general risk management strategies related to data security, confidentiality, and privacy.

1. Become familiar with published guidelines. HIPAA compliance is a set of processes rather than a defined set of rules. As such, technical requirements are not always absolute. However, existing guidelines offer specifics on appropriate technology to use and methods to safeguard data (Turvey et al., 2013; Yellowlees, Shore, et al., 2010).
2. Obtain training, at least a basic technical knowledge of the systems both patients and providers will use. Also, know where to seek the help of technical experts to assist with any patient privacy and data security concerns that may arise. These steps might help mitigate risk for liability over possible negligence for failure to operate the technology appropriately.
3. Know HIPAA, but also know state privacy laws, as compliance with HIPAA alone may not fully suffice to ensure maximum privacy and security. While HIPAA will likely preempt state laws that have less stringent privacy and security requirements, state laws that have more stringent privacy and security requirements might preempt HIPAA (Genomics Law Report, 2011; Hyler & Gangure, 2004).

Ultimately, TMH providers should feel comfortable that any electronic means chosen to communicate or exchange information with patients is sufficient enough to allow them to make accurate clinical decisions. If not, they may fall short of proving an accepted standard of care. While there may be initial uncertainty as to how to most effectively safeguard these issues, the above considerations should help to ease concerns. In sum, it is important for the TMH professional to use approved technologies, know the privacy requirements for their use, and remain aware of potential liability issues related to use of technology.

Safety Plans and Emergency Management

Given that the use of technology to deliver mental health care provides some unique clinical situations, having an established plan for dealing with technical, medical, and clinical emergencies is a necessary risk management strategy, and is required in most standard operating procedures and manuals. Some industry guidelines provide specific recommendations for managing emergencies (Turvey et al., 2013; Yellowlees, Shore, et al., 2010) that can help establish an individual safety plan. Given potential problems with the technology and network infrastructure (e.g., lost connection, poor quality of communication via the technology) it is essential that the TMH clinician have a secondary method for immediately contacting the patient and/or staff at the patient site.

As part of a safety plan the provider needs to obtain knowledge of patient site civil commitment laws and *Tarasoff* type duty to warn/protect requirements since procedures for hospitalization and duty to warn requirements vary by jurisdiction (Godleski, Nieves, Darkins, & Lehmann, 2008; Turvey et al., 2013). While more than half of the individual states in the United States have enacted statutes for mandatory duty to warn, they vary in how they specify who can be warned (law enforcement and/or the intended victim) and to how much discretion the clinician has in applying his or her own judgment to the case. In addition, several states and the District of Columbia give permission to warn but do not impose duty to warn. And finally, within states that have no duty to warn statutes: some have case law that imposes a duty, while others have no clear case law or statute on the topic. Not knowing the proper local law or regulation to follow in case of an emergency can open one up to potential liability. But as with other areas, obtaining information relevant to one's specific situation and jurisdiction is an effective risk management strategy (Herbert, 2002; Walcott, Cerundolo, & Beck, 2001).

Risk Management in Home-Based TMH

The provision of TMH care to clinically unsupervised settings, such as to a patient's home, continues to grow with many seeing the potential for in-home TMH care to improve access for those unable or unwilling to seek traditional mental health care due to barriers associated with mobility, geography, or concerns about stigma (Luxton et al., in press). Although there has been limited empirical investigation into these types of settings, guidelines that have addressed procedures for safe provision of in-home care (Gros et al., 2011; Luxton et al., in press; Shore, Hilty, & Yellowlees, 2007; Shore, 2011; Turvey et al., 2013) and a recent review article (Luxton, Sirotin, & Mishkind, 2010) provide initial indication that in-home TMH care can be safely managed. A consistent suggestion is to have a local collaborator or second care provider supply an additional method for contacting patients or authorities in case of technical, medical, or clinical emergency; these collaborators may also provide technical assistance if a connection is lost or assist with transportation (if necessary) to the appropriate place during an emergency. We want to emphasize it is expected that in-home care will continue to grow as large federal agencies like the VA are already providing in-home TMH care.

Mobile Health

Mobile health, sometimes abbreviated as mHealth, is usually defined broadly to include any promotion of health using mobile devices or wireless technology (World Health Organization, 2011). In other words, using a smartphone or tablet computer to track calories, look up medical symptoms, or send information to a provider is engaging in mobile health. While synchronous care is technologically possible, much of mobile health focuses on asynchronous care (not occurring in real time between provider and patient) such that the patient is primarily interacting with a mobile device. As a result of this different dynamic, incorporating mobile health into a treatment regimen can provide additional legal and regulatory challenges. We review some of the primary issues below and provide some practical recommendations to help mitigate risk and concern over using mobile health, as it can offer great patient benefits.

As the use of health-based mobile apps (applications) increases, there are growing regulatory concerns over how to best protect patients who might use apps on their own, and make decisions on information contained in apps without direct clinical oversight. There is no regulatory process for all mobile health applications, including mobile apps or websites, and anyone can publish a website or mobile app and claim that the services and information within promote health. As such, it is essential that providers be cognizant of the health apps and sites used by patients. An initial good practice recommendation is to stay current on apps or websites that patients may visit. Certainly it is critical to become thoroughly familiar with the content and, if available, research, on any app or website one might recommend to a patient. Although it is unclear if this would shield one from all liability if a patient were to use an app you recommended and suffered an injury as a result, it at least allows one to use good clinical judgment in any care-related recommendations, and hopefully avoid recommending an app that one has concerns about for any reason.

Because much of mobile health entails a patient interacting with a mobile device, advance thought and caution must be given to the best ways to store and assess patient data sent from mobile health applications. As discussed by Luxton, Kayl, et al. (2012), there are a number of particular issues that threaten privacy and the security of patient data with the use of these devices, notably their wireless capabilities. Although the ability to exchange electronic data (via mobile app, cell phone, or email) to a treating provider is valuable, there are a couple of potential legal questions to consider: (a) How does the provider receive and store the data in a HIPAA compliant manner? (b) What should the provider do if the patient sends data that indicates potential for harm to self or others? HIPAA applies to "covered entities" and their associates. Patients are generally not "covered entities." In other words, patients can do whatever they choose with their own data. If the patient transmits or shares any electronic protected health care information (PHI) with a health care professional who is a covered HIPAA entity, then the health care professional becomes responsible for HIPAA compliance (Luxton, McCann, Bush, Mishkind, & Reger, 2011). Clearly this places a burden on the provider.

The first issue relevant to mobile applications then is the level of security of any health information a patient may transmit to a provider. If a provider is receiving this information on a cell phone, this is a potential concern because many cell phones may not use adequate security measures to prevent third party attack or interception of data. For example, use of wireless technology, such as Wi-Fi and cellular networks, can make it easier for third parties to monitor and record unencrypted data than it is with hard-wired networks. Although current security standards such as Wi-Fi Protected Access exist, there is no guarantee that the end user (often the provider) has enabled these security features or whether they are in place in public environments. Ultimately, electronic data must be encrypted before transmission in order to prevent threats to privacy in most wireless environments; ensuring use of HIPAA compliant encryptions features on one's smartphone is the best approach (Luxton, Kayl, et al., 2012; Luxton, O'Brien, McCann and Mishkind, 2012). What happens when data are maintained on a mobile phone and the device is lost or stolen? It seems best to take precautions with any patient data received in any electronic form (on a mobile phone, by email, on a website) and to securely transfer and store that information as if it were any other document, and then delete the electronic communication so that it is no longer living (i.e., stored) on the server—the virtual database. Although a smartphone and email system may be highly secure, it will be easier to monitor the lifespan of the Protected Health Information (PHI) if it is integrated into the patient record so that it is destroyed at the correct time.

Prevention is the key to avoiding the second issue: the case of a patient sending data that indicates potential for harm to self or others. First consider a voicemail system and the limits to that modality. On voicemail greetings, providers can indicate how frequently they check voicemail, refer patients needing immediate attention to the emergency department of a local hospital, or use language such as "if this is an emergency, please hang up and dial 911." This way the patient is notified *prior to leaving a voicemail recording* that a provider may or may not hear the message soon and there is an alternate option for immediate support if needed. With email, providers can similarly set an automatic response with similar

information that is immediately sent to all individuals who send email to the account. Because this email response is sent *after* the patient has emailed, it is not quite the same as the case of a voicemail (in which a patient hears all caveats prior to leaving a message). For this reason, it is again essential to discuss the limits of email communication in person with a patient and then clearly indicate this conversation in session notes. As discussed above, informed consent procedures and details can help mitigate risk. If email communication is used regularly, consider adapting consent for treatment forms with a space for the patient to initial that he or she understands that "this email box is monitored every ____ hours, except on weekends. You may or may not receive a response within ____ hours."

One aspect of mobile health that is now subject to regulatory scrutiny is any mobile medical app that falls into the Food and Drug Administration's (FDA) definition of a medical device "whose functionality could pose a risk to a patient's safety if the mobile app were not to function as intended" (FDA, 2013). The FDA considers a medical device to be a product intended to prevent or treat any aspect of human functioning and defines it in section 201(h) of the Federal Food, Drug, and Cosmetic Act. In order for a mobile medical application to fall under current FDA regulation it must meet this definition and be intended (a) to be used as an accessory to an already regulated medical device, or (b) to transform a mobile communication device into a regulated medical device (FDA, 2013). The FDA was clear to state that not all mobile apps will meet this criteria and that they are not interested in regulating apps that pose a low risk of harm to the public. The FDA guidance provides numerous examples of types of mobile apps that it does not intend to enforce (will "exercise enforcement discretion"), and it is likely that many, though not all, mental health apps fall into this category. The list of categories of apps that the FDA does and does not intend to regulate is somewhat detailed, and too long to repeat here, but does warrant review. Because these regulations were adopted recently (September, 2013), it is unclear how the regulatory process will affect the apps currently deployed to market that are subject to regulation. It is recommended that any TMH practitioner who may wish to use mobile apps in their practice with patients become familiar with this regulatory guidance.

There are a couple of additional key points to consider from the FDA guidance. One, the focus of the regulatory authority is over those that "manufacture" mobile apps, and not those that simply use them. The FDA guidance states "licensed practitioners ... who manufacture a mobile medical app or alter a mobile medical app solely for use in their professional practice and do not label or promote their mobile medical apps to be generally used by other licensed practitioners or other individuals" (FDA, 2103, p. 11) as those *not* meeting the definition of manufacturer, and thus not under regulation. This seems to exclude from FDA regulation, any mental health practitioner who simply recommends an app to a patient to use as part of care. This would suggest that from a regulatory standpoint, mental health clinicians should not hesitate to recommend to patients use of any mobile application they feel can improve patient care. A second note is that the FDA is expected to release further guidance in 2014 on "software that performs patient-specific analysis to aid or support clinical decision-making." These regulations will be deployed as part of a congressionally mandated plan for regulation for health information technology and may increase scrutiny on mobile health apps and websites.

In summary, mobile health applications can be safely integrated into standard treatment and recommended to patients for self-care use. The regulatory environment for use of mobile health applications in mental health is in its infancy, with many issues to consider and more that may emerge (see Schulke, 2013, for a legal review of the mobile health regulatory arena).

Social Networking

Social networking refers to the use of social forms of media, such as websites, blogs, and other software, to connect with other users who may or may not be known to the individual outside of the online context. Common examples of social networking include websites such as Facebook and LinkedIn, blogs, Twitter, and video sharing sites. In addition to engaging in social networking for personal use, many providers now have websites that include mental health blogs and Facebook pages with health tips. These forms of social networking allow the provider to covertly market their services by building a social media "platform." Although economical and efficient, social media use in mental health practice can easily cross privacy or ethical lines.

Although there is currently no specific regulation for mental health providers who engage in social networking for professional or personal use, there are potential malpractice and licensure complaints that could occur with use of social media, most likely with the inappropriate disclosure of patient information or the inappropriate "marketing" of oneself. Ensuring privacy and confidentiality are the primary risk management strategies to consider when using social media, while maintaining professional boundaries and establishing clear expectations regarding communication over social media are the primary ethical issues to consider. To help maintain provider privacy, some clinicians have two sets of social media accounts: one set for professional life and one for personal. For example, a provider's website may include a blog or an icon to "like" the clinic on Facebook or other social media outlets. In

addition, many providers use profiles on regional or national association websites in order to accrue business. Of course, providers should use common sense when setting up these accounts to use only professional email addresses and other contact information. However, even when following this precaution, providers must remain vigilant about these accounts to ensure that they do not accidentally cross over with personal ones. In addition, some providers now integrate a social media policy into the regular intake and informed consent procedure. This is a clear statement of how the provider uses social media, and how he or she will (or won't) engage with patients outside the confines of the therapy sessions. For example, a social media policy could clearly explain that a provider does not regularly check messages on social media platforms, and does not engage in any communication with patients outside of face-to-face sessions, telephone, or professional email accounts. This type of policy can protect both the patient and the provider: patients will be socialized to appropriate online engagement with their clinicians, and providers can refer back to the policy later if the patient attempts to seek care via an inappropriate channel. As with other issues discussed in this article, clear explanation of policies and expectations regarding use of technology at initial patient communication is vital.

Conclusion

This article was designed to provide an overview of some regulatory considerations associated with the safe and effective delivery of mental health services using telecommunications technologies. While it is important to be aware of these issues, the overarching principles for providing good clinical care using established practice standards for the broader mental health field remain the core of safe and effective practice. With this article we have tried to alleviate common concerns and remove some hesitancy about the delivery of mental health care using technologies. The information and recommendations presented should give any new or seasoned provider the foundation necessary to effectively mitigate any real or perceived risk associated with TMH care. We also hope that knowledge of the TMH specific issues and the risk management strategies discussed will allow all telehealth stakeholders to feel more comfortable about using technology to deliver and receive mental health care.

Telemental health is a dynamic field and it is a very exciting time to be not just a part of but also a driver of its growth. As technology expands, so does the opportunity to deliver TMH services in new ways and to more patient-accessible locations. This in turn offers individuals in the field the possibility to build something new, and to be on the cutting edge of developing standards and regulations that will govern health care delivery into the future. This dynamism will require stakeholders to remain current and up-to-date on TMH issues so that they may continue to advance the field. We hope we have provided this background and look forward to continuing to work with others to appropriately grow the field.

References

American Psychiatric Association. (1998). *Telepsychiatry via videoconferencing*. Retrieved from http://www.telepsychiatry.com/apa.pdf

American Psychological Association. (2010). *Practice Directorate, Legal & Regulatory Affairs. Telehealth 50-state review*. Retrieved from http://www.apapracticecentral.org/advocacy/state/telehealth-slides.pdf

American Psychological Association Practice Organization. (2010). Telehealth: Legal basics for psychologists. *Good Practice* Available to members of the APA Practice Organization at: http://www.apapracticecentral.org/update/2010/08-31/telehealth-resources.aspx

American Telemedicine Association. (2013). *State telemedicine legislation tracking*. Retrieved from http://www.americantelemed.org/docs/default-source/policy/state-telemedicine-legislation-matrix.pdf.

Ameringer, C. F. (2011). State-based licensure of telemedicine: The need for uniformity but not a national scheme. *Journal of Health Care Law & Policy*, *14*, 55–85. Retrieved from http://digitalcommons.law.umaryland.edu/jhclp/vol14/iss1/3

Backhaus, A., Agha, Z., Maglione, M. L., Repp, A., Ross, B., Zuest, D., . . .Thorp, S. R. (2012). Videoconferencing psychotherapy: A systematic review. *Psychological Services*, *9*(2), 111–131. http://dx.doi.org/10.1037/a0027924

Brooks, E., Turvey, C., & Augusterfer, E. F. (2013). Provider barriers to telemental health: Obstacles overcome, obstacles remaining. *Telemedicine and e-Health*, *19*(6), 433–437. http://dx.doi.org/10.1089/tmj.2013.0068

Centers for Medicare and Medicaid.U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Retrieved November 2, 2013, from http://www.cms.hhs.gov/HIPAAGenInfo.

Changes Affecting Hospital and Critical Access Hospital Conditions of Participation: Telemedicine Credentialing and Privileging, 42 CFR (Code of Federal Regulations) Part 482 and 485(2011)

Chee, J. (2010). *Center for Telehealth & e-Health Law. Tele-medical malpractice: Negligence in the practice of telemedicine and related issues*. Retrieved from http://www.ctel.org/research/TeleMedical%20Malpractice%20Negligence%20in%20the%20Practice%20of%20Telemedicine%20and%20Related%20Issues.pdf.

Darkins, A., Foster, L., Anderson, C., Goldschmidt, L., & Selvin, G. (2013). The design, implementation, and operational management of a comprehensive quality management program to support national telehealth networks. *Telemedicine and e-Health*, *19*(7), 557–564. http://dx.doi.org/10.1089/tmj.2012.0263.

Fleisher, L. D., & Dechene, J. C. (2004). *Telemedicine and e-health law*. New York: Law Journal Press.

Food and Drug Administration. (2013). *Mobile medical applications - Guidance for industry and food and drug administration staff*. Retrieved from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

Genomics Law Report. (2011). Don't forget about state law: Michigan decision reminds health care providers of HIPAA preemption issue. *Isidore Steiner, DPM, PC v. Marc Bonanni*, No. 294016 (Mich. Ct. App. Apr. 7, 2011). Retrieved from http://www.genomicslawreport.com/index.php/2011/06/28/dont-forget-about-state-law-michigan-decision-reminds-health-care-providers-of-hipaa-preemption-issue.

Godleski, L., Nieves, J. E., Darkins, A., & Lehmann, L. (2008). VA telemental health: Suicide assessment. *Behavioral Sciences and the Law*, *26*, 271–286. http://dx.doi.org/10.1002/bsl.811

Grady, B., Myers, K. M., Nelson, E. L., Belz, N., Bennett, L., Carnahan, L., . . . Voyles, D. (2011). Evidence-based practice for telemental health. *Telemedicine Journal and e-Health*, *17*, 131–148. http://dx.doi.org/10.1089/tmj.2010.0158

Gros, D. F., Veronee, K., Strachan, M., Ruggerio, K. J., & Acierno, R. (2011). Managing suicidality in home-based telehealth. *Journal of Telemedicine and Telecare, 17*, 332–335. http://dx.doi.org/10.1258/jtt.2011.101207

Gupta, A., & Soa, D. (2010). The unconstitutionality of current legal barriers to telemedicine in the United States: Analysis and future directions of its relationship to national and international health care reform.*Health Matrix: Journal of Law-Medicine*. Retrieved from the Social Science Research Network at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1549765.

H.R. 6353–110th Congress: Ryan Haight Online Pharmacy Consumer Protection Act of 2008. Retrieved from http://www.govtrack.us/congress/bills/110/hr6353

Hageseth v. Superior Court,150 Cal. App. 4th 1399 (2007).

Herbert, P. B. (2002). The duty to warn: A reconsideration and critique. *Journal of the American Academy of Psychiatry and the Law*, 30, 417–424. Retrieved from http://www.jaapl.org/content/30/3/417.full.pdf

Hilty, D. M., Ferrer, D. C., Parish, M. B., Johnston, B., Callahan, E. J., & Yellowlees, P. M. (2013). The effectiveness of telemental health: A 2013 review. *Telemedicine Journal and e-Health*, 19(6), 444–454. http://dx.doi.org/10.1089/tmj.2013.0075.

Hyler, S. E., & Gangure, D. P. (2004). Legal and ethical challenges in telepsychiatry. *Journal of Psychiatric Practice, 10*, 272–276.

Joint Commission Perspectives. (2012). *Accepted: Final revisions to telemedicine standards*. Retrieved from http://www.jointcommission.org/assets/1/6/Revisions_telemedicine_standards.pdf.

Kramer, G. K., Ayers, T., Mishkind, M., & Norem, A. (2011). *DoD telemental health guidebook*. National Center for Telehealth and Technology. Retrieved from http://t2health.org/sites/default/files/cth/guidebook/tmh-guidebook_06-11.pdf.

Kramer, G. M., Mishkind, M. C., Luxton, D. D., & Shore, J. H. (2012). Managing risk and protecting privacy in telemental health: An overview of legal, regulatory, and risk management issues. In K. Myers & C. Turvey (Eds.), *Telemental health: Clinical, technical and administrative foundations for evidence-based practice*. New York: Elsevier.

Luxton, D. D., Kayl, R. A., & Mishkind, M. C. (2012). mHealth data security: The need for HIPAA-compliant standardization. *Telemedicine and e-Health, 18*(4), 284–288. http://dx.doi.org/10.1089/tmj.2011.0180

Luxton, D. D., McCann, R. A., Bush, N. E., Mishkind, M. C., & Reger, G. M. (2011). mHealth for mental health: Integrating smartphone technology in behavioral healthcare. *Professional Psychology: Research & Practice, 42*, 505–512. http://dx.doi.org/10.1037/a0024485

Luxton, D. D., O'Brien, K., McCann, R. A., & Mishkind, M. C. (2012). Home-based telemental healthcare safety planning: What you need to know. *Telemedicine and e-Health, 18*(8), 629–633. http://dx.doi.org/10.1089/tmj.2012.0004

Luxton, D. D., Sirotin, A. P., & Mishkind, M. C. (2010). Safety of telemental health care delivered to clinically unsupervised settings: A systematic review. *Telemedicine and e-Health, 16*, 705–711. http://dx.doi.org/10.1089/tmj.2009.0179

Luxton, D. D., O'Brien, K., Pruitt, L. D., Johnson, K., & Kramer, G. (2014). *Managing suicide risk in home-based telepractice, International Journal of Psychiatry in Medicine*. (in press).

Miller, T. W., Burton, D. C., Hill, K., Luftman, G., Veltkemp, L. J., & Swope, M. (2005). Telepsychiatry: Critical dimensions for forensic services. *Journal of the American Academy of Psychiatry and the Law, 33*, 539–546.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 FR 5565 (2013). Retrieved from. http://www.gpo.gov/fdsys/granule/FR-2013-01-25/2013-01073/content-detail.html

Myers, K., & Cain, S. (2008). Practice parameter for telepsychiatry with children and adolescents. *Journal of American Academy of Child and Adolescent Psychiatry, 47*, 1468–1483. http://dx.doi.org/10.1097/CHI.0b013e31818b4e13

Natoli, C. M. (2009). *Summary of findings: Malpractice and telemedicine.*: Center for Telehealth & e-Health Law (Retrieved from http://www.ctel.org/research/Summary%20of%20Findings%20Malpractice%20and%20Telemedicine.pdf).

Natoli, C. M. (2011). *Telemedicine: Prescribing and the Internet*. Center for Telehealth & e-ealth Law. Retrieved from http://ctel.org/wp-content/uploads/2011/06/Telemedicine-Prescribing-and-the-Internet.pdf.

Odor, A., Yellowlees, P., Hilty, D., Parish, M. B., Nafiz, N., & Iosif, A. M. (2011). PsychVACS: A system for asynchronous telepsychiatry. *Telemedicine and e-Health*, 17(4), 299–303. http://dx.doi.org/10.1089/tmj.2010.0159.

Ohio Psychological Association. (2009). *Telepsychology guidelines*. Retrieved from http://www.ohpsych.org/psychologists/files/2011/06/OPATelepsychologyGuidelines41710.pdf

Petzel, R. A. (2013). *Telemental health in VA: A new source of support for veterans*. Retrieved from http://www.usmedicine.com/outlook/telemental-health-in-va-a-new-source-of-support-for-veterans.html?page=1

Poropatich, R., Lai, E., McVeigh, F., & Bashshur, R. (2013). The U.S. Army telemedicine and m-Health program: Making a difference at home and abroad. *Telemedicine and e-Health, 19*(5), 380–386. http://dx.doi.org/10.1089/tmj.2012.0297

Richardson, L. K., Frueh, B. C., Grubaugh, A. L., Egede, L., & Elhai, J. D. (2009). Current Directions in Videoconferencing Tele-Mental Health Research.*Clinical Psychology (New York)*. 1; 16–323–338.

Schulke, D. F. (2013). The regulatory arms race: Mobile health applications and agency posturing. *Boston University Law Review*, 93, 1699–1752.

Shore, J. H., Hilty, D. M., & Yellowlees, P. (2007). Emergency management guidelines for telepsychiatry. *General Hospital Psychiatry*, 29, 199–206.

Shore, P. (2011). *VISN 20 Home Based Telemental Health Pilot Program Standard Operating Procedures Manual*. Portland, OR: Veteran's Health Administration.

Steinhubl, S. R., Muse, E. D., & Topol, E. J. (2013). Can mobile health technologies transform health care? *Journal of the American Medical Association*. http://dx.doi.org/10.1001/jama.2013.281078.

Turvey, C., Coleman, M., Dennison, O., Drude, K., Goldenson, M., Hirsch, P., . . .Bernard, J. (2013). ATA Practice Guidelines for Video-Based Online Mental Health Services. *Telemedicine and e-Health*, 19(9), 722–730. http://dx.doi.org/10.1089/tmj.2013.9989.

U.S. Constitution, Amendment X.

U.S. Department of Health and Human Services. Health Insurance Portabilityand Accountability Act of 1996 (HIPAA). Retrieved from www.cms.hhs.gov/HIPAAGenInfo

U.S. Department of Health and Human Services, & Health Resources and Services Administration (2010). *Health Licensing Board, Report to Congress*. Retrieved from http://www.hrsa.gov/ruralhealth/about/telehealth/licenserpt10.pdf.

Walcott, D. M., Cerundolo, P. Beck, J. C. (2001). Current analysis of the Tarasoff Duty: An evolution towards the limitation of the duty to protect. *Behavioral Sciences and the Law, 19*, 325–343.

World Health Organization. (2011). mHealth new horizons forhealth through mobile technologies. *Global observatory for eHealth series*, (Vol. 3).Geneva, Switzerland: WHO Press.

Yellowlees, P. M., Odor, A., Parish, M. B., Iosif, A. M., Haught, K., & Hilty, D. (2010). A feasibility study of the use of asynchronous-telepsychiatry for psychiatric consultations. *Psychiatric Services, 61*(8), 838–840. http://dx.doi.org/10.1176/appi.ps.61.8.838.

Yellowlees, P., Shore, J., & Roberts, L. (2010). Practice Guidelines for Videoconferencing-Based Telemental Health - October 2009. *Telemedicine and e-Health, 16*(10), 1074–1089. http://dx.doi.org/10.1089/tmj.2010.0148

DISCLAIMER: Any opinions or assertions contained herein are the private views of the authors and are not to be construed as official or reflecting the views of the Department of the Army or the Department of Defense.

Address correspondence to Matt C. Mishkind, Ph.D., National Center for Telehealth and Technology, 9933 West Hayes Street, Joint Base Lewis-McChord, WA, 98431; e-mail: matthew.c.mishkind.civ@mail.mil.

Received: December 17, 2013
Accepted: April 23, 2014
Available online 2 June 2014