<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2020 D&amp;O Symposium</td>
</tr>
<tr>
<td>4</td>
<td>PLUS Foundation Scholarship Programs</td>
</tr>
<tr>
<td>5</td>
<td>Artificial Intelligence in Healthcare: A New Frontier in Coverage &amp; Liability</td>
</tr>
<tr>
<td>8</td>
<td>Telemedicine: Regulatory and Liability Trends</td>
</tr>
<tr>
<td>17</td>
<td>Strikes for Charity</td>
</tr>
<tr>
<td>18</td>
<td>2019 PLUS Conference Event Recap</td>
</tr>
<tr>
<td>23</td>
<td>New Regulation Best Interest Becomes Effective for Broker Dealers</td>
</tr>
<tr>
<td>27</td>
<td>Surprise! There’s a Trial Next Week</td>
</tr>
<tr>
<td>30</td>
<td>Foundation Scholarships</td>
</tr>
<tr>
<td>31</td>
<td>2020 Cyber Symposium</td>
</tr>
</tbody>
</table>
UNCOVER THE TRENDS.

DISCOVER THE INSIGHTS.

CONNECT WITH THE EXPERTS.

2020 PLUS D&O SYMPOSIUM

FEB. 25-26 NEW YORK, NY

WWW.PLUSWEB.ORG/EVENTS
Applications are being accepted for the 2020 PLUS Foundation Scholarship Programs. Scholarships are available to any college-bound children of PLUS members or corporate sponsor company employees, and are offered in two separate programs, Financial Aid and Gilmartin.

**APPLICATION DEADLINE: FRIDAY, JANUARY 31, 2020**

**GENERAL DETAILS & REQUIREMENTS FOR BOTH SCHOLARSHIP PROGRAMS**

- Up to four scholarships will be awarded in each program (Gilmartin, Financial Aid)
- Scholarships will be for up to $12,000 each, payable in increments over four years
- Applicants must be a child of a current PLUS member or a child of an employee of a current PLUS corporate sponsor
- Applicants are required to be in their senior year of high school
- Recipients must successfully complete high school and enroll in an accredited four year college or university in the fall of 2020
- A student may apply for both scholarships, but can only be awarded one

Financial aid scholarships made possible by the personal donations of leaders in our industry:

- James E. Price Memorial Scholarship
- Elizabeth Everson Seyler & Mary Quayle Bradley Scholarship
- Mary Dortenzio Memorial Scholarship

For complete information and a link to the online application, go to [www.PLUSFoundation.org](http://www.PLUSFoundation.org)
It’s used to drive cars, pick stocks, and even ensure you never run out of your favorite laundry detergent. Today, artificial intelligence (AI) is being utilized across most industries and has increasingly become a part of people’s daily lives, but its use to diagnose, treat, and otherwise facilitate care for patients in the healthcare setting raises unique legal concerns.

To be clear, artificial intelligence is currently being used in healthcare and its use will only increase as companies continue investing in the development of these “ultra-smart” technologies. As such, it is important to consider a pressing legal question: how will novel liability issues arising from the use of AI in healthcare be addressed?

The Use of AI in Healthcare

AI is an assortment of technologies, including machine learning, natural language processing, and expert systems, and plays a variety of roles in the healthcare setting. For example, IBM’s Watson Computer system utilizes a “question and answer” methodology to support clinical decision making. In doing so, a physician is able to pose a question to Watson and describe a variety of patient-specific factors (such as symptoms and treatment history). Watson then sifts through an extensive amount of data and supplies the physician with responsive hypotheses and recommendations. Through a process of continual data input, Watson is able to “learn” and improve its future recommendations.

Machine learning is also being used to prescribe accurate doses of Warfarin, an anticoagulant that is known to cause
adverse drug events if not properly dose prescribed. Some electronic health record software systems are likewise utilizing AI, which can read and parse natural language in medical transcripts to select vital medical information from those transcripts and transfer that information into specific locations in patients’ electronic health record.

Chatbots are AI-driven computer programs that simulate human dialogue through voice and/or text conversations, and are being used as a way to provide initial consultation services. Most notably, in July 2019, the United Kingdom’s National Health Service (NHS) announced a partnership with Amazon’s Alexa. Now, UK-based patients are able to receive health advice from Alexa through the NHS website.

In addition to playing a supportive role, physicians and healthcare organizations are utilizing AI to clinically diagnose patients. For instance, the Food and Drug Administration has approved an AI-driven device that can detect signs of diabetic blindness. Similar applications of AI are being used in radiology to detect cancerous tissues seen on MRI and CT scans and rare diseases through facial recognition software. Although these diagnoses are confirmed by a physician, it’s easy to imagine a future where AI diagnoses are made with limited or no physician oversight.

AI’s Impact on Liability

The most common source of liability in healthcare is medical negligence that results in an injury. Under tort law, liability arising out of medical negligence with the use of a medical device is typically dealt with in three ways. First, a physician can be held liable under a theory of negligence/malpractice if it is determined that the physician’s actions fell below what would be expected of a “reasonable physician.” Second, a healthcare organization can be held liable under a theory of respondeat superior for the negligence of its employees that occurs “within the scope of their employment” or for failing to adequately supervise, train or hire its employees. Third, medical device manufacturers can be held liable under a theory of products liability if their products are not “reasonably safe” as a result of a manufacturing defect, design defect, or an inadequate warning. In the healthcare setting, products liability comes with a unique twist: according to the learned intermediary doctrine, a patient who is harmed by a medical device typically cannot sue the device’s manufacturer directly, as the physician is considered to have the responsibility to adequately warn the patient regarding the risks associated with the use of the device.

The integration of AI into healthcare and the increasing autonomy of AI-driven systems upends this medical liability analysis. For instance, a physician’s reliance on a machine learning system that results in a misdiagnosis, medication error, or unnecessary procedure could amount to negligence. In this situation, however, it may be difficult to assign legal responsibility for the negligence, especially given the lack of clarity regarding how the AI system analyzed its data and arrived at its conclusion. Moreover, the limitations on the relief available from the AI developers further complicates this matter, as AI is increasingly being used to provide direct clinical care to patients. Even if patients could seek relief from the developers of an AI system, it would arguably be inequitable to assign liability to the designers for the decisions made by the AI system that were the result of the system’s interpretation of data, as opposed to a design defect.

When it comes to a dispute about liability between a technology service provider and a healthcare organization, the contract between the entities will generally govern the apportionment of liability. Generally, a technology services contract limits the liability of the technology service provider. Again however, the reliance on AI as a tool to provide direct patient care, as opposed to a tool to support clinical decision making, may make it more difficult for technology service providers to continue to limit their liability in this way.

In addition to medical negligence, the use of AI in healthcare raises a variety of cyber liability issues. One of the primary concerns that arise from the increased use of technology in the clinical setting is the ability for an unauthorized third-party to gain access to the technology and utilize it for nefarious purposes. In the context of AI, the ability to access the AI algorithms could result in misdiagnosis and other patient harm. The use of AI-driven communication systems such as chatbots also triggers data privacy considerations. Medical data is one of the most sensitive forms of data making it highly sought after and lucrative on the black market. As such, the medical information provided by patients to chatbots or other AI consultation devices will certainly be targeted by cyber criminals. Regardless of the type of device that receives the data, it is the responsibility of the healthcare organization to ensure the protection of its patients’ data.
Insurance Implications

One of the primary ways physicians and healthcare organizations address the liability they face is through the purchase of insurance. While there are robust insurance products that address liability arising in the healthcare context, few of these products specifically contemplate the use of AI.

In a typical medical negligence scenario, if a patient alleges that he was harmed as a result of the actions of a physician, a medical malpractice insurance policy would likely respond to provide coverage. The intervention of an AI-driven system in the physician’s decision-making process, however, may muddy this equation and could limit the amount of coverage available. Similarly, if a technology service provider is sued due to the failure of its product to operate properly, a technology errors and omissions insurance policy (which may be purchased as a standalone policy or as part of a comprehensive cyber liability policy) would likely provide coverage.

If, however, the lawsuit is based upon bodily injury caused by the service provider’s product—in this case an AI-driven system—a bodily injury exclusion may operate to deny coverage. Although the service provider may have purchased bodily injury coverage under a general liability policy, such a policy would likely have an exclusion for a bodily injury that was the result of the service provider’s professional services (i.e., providing the AI-driven system to the healthcare organization). Thus, this type of lawsuit could potentially fall through the cracks of coverage, leaving the service provider responsible for the costs associated with its defense.

The availability of coverage for cyber claims arising from the use of AI in healthcare is similarly complex. While a healthcare organization may have coverage under a cyber liability policy if an unauthorized third-party accesses an AI-driven system on its computer network, such coverage may be unavailable if the unauthorized access results in bodily injury (again, due to a bodily injury exclusion). In addition, although it is a healthcare organization’s responsibility to protect its patients’ data, the use of AI may result in a portion of the data being maintained by a third-party. If the third-party vendor allows the healthcare organization’s data to be accessed, the healthcare organization can still be held liable. In such a scenario, coverage complications could arise unless the healthcare organization’s cyber liability policy expressly extends coverage for data being maintained on computer systems that are operated and maintained “on behalf of” the organization by a third-party.

Looking Forward

Without question, the use of AI in healthcare has the potential to improve patient outcomes and create efficiencies across the healthcare industry. Along with those benefits come novel liability concepts. Liability and coverage lawsuits arising out of the use of AI in healthcare are likely, especially as the case law in this area is in its infancy. As discussed above, the current legal standards appear insufficient to address these issues. Accordingly, new legal and regulatory frameworks may be needed to provide clarity with respect to the obligations and liabilities associated with AI. Similarly, in order to facilitate the continued use of AI in healthcare, insurance products will need to evolve to specifically contemplate the ramifications of AI and thereby provide the necessary coverage.

ABOUT THE AUTHORS

BETSY D. BAYDALA, ESQ. is a partner at Kaufman Borgeest & Ryan LLP practicing in the firm’s Cyber Liability, Medical Malpractice, and Healthcare groups.

HARRISON M. COVALL, ESQ. is an associate attorney at Kaufman Borgeest & Ryan LLP specializing in cyber liability coverage matters and has served as coverage counsel in connection with several large, complex data breaches. He has also served as coverage counsel in connection with a variety of privacy law matters arising under state and federal regulations, including the Telephone Consumer Protection Act and the California Invasion of Privacy Act. Additionally, Harrison has experience counseling clients on cyber/data privacy issues, including their obligations under HIPAA/HITECH, and other regulatory compliance issues. Harrison regularly speaks on the topic of cyber liability, with a particular focus on the healthcare industry.
Introduction

There has been a rapid adoption of telemedicine and telehealth technology in the United States over the last decade. In this article we briefly review the growth of telemedicine and telehealth technology and examine some of the main regulatory and liability considerations pertinent to insuring and managing the risk of health care services arising out of a patient-provider video encounter, what we will deem “classic telemedicine”. The goal is to provide an overview of the growth of telemedicine/telehealth, the types of telemedicine and telehealth technologies in common use today, and applicable regulatory and legal issues pertinent to medical professional liability.

The Growth of Telemedicine/Telehealth

Major factors that have driven the growth of telemedicine and telehealth include lower cost: patient demand; better acceptance for reimbursement by payers; and a more favorable regulatory environment.1 There also have been great strides in the development of telemedicine and telehealth technology.2

The ongoing investment in new digital telehealth technology is in the billions of dollars. There were 7 million patient encounters via telemedicine in 2018 and this number is expected to almost triple by 2020 and to continue to increase dramatically in the years ahead.3 Telemedicine provides two key advantages in delivering care: lower cost and easier patient access - convenience.4
Telemedicine/telehealth has been adopted by many medical specialties and many types of facilities, especially hospitals. Examples of patient-physician video encounters can best be seen in the primary care specialties of internal medicine, family practice and pediatrics, as well as in psychiatry and neurology (especially stroke care), but utilization goes well beyond those disciplines. Telehealth technology allows for remote diagnosis and improved care in such specialties as radiology, cardiology, obstetrics, dermatology, pathology and many others.5

Many hospitals and health care systems as well as physician groups are beginning to use telemedicine for follow-up visits after surgery6 as well as for helping patients manage chronic conditions such as heart failure or diabetes through remote monitoring as well as video encounters.7 Telemedicine offers promise for treating substance use disorder and thereby helping address the opioid problem.8

**Telemedicine and Telehealth**

It is not easy to define the terms telemedicine and telehealth and they are sometimes used interchangeably. “Telemedicine” has at least 100 definitions in peer-reviewed publications. It has been around longer than “telehealth.” For our purposes in this article, “telemedicine” can be thought of as the patient-provider video encounter. But many think telemedicine came into its own through teleradiology, sending films and scans across state lines and even across international borders.

Telemedicine is defined by the American Telemedicine Association as “the use of medical information exchanged from one site to another via electronic communications to improve patients’ health status.”9 “Telehealth” is a broader term that encompasses the many and varied applications of distance care technology, often consumer facing, in a rapidly evolving health care environment.10 The increasing emphasis on care management, particularly for patients with chronic conditions, and the focus on health and wellness for disease management and prevention all fall within the purview of telehealth.

**Telehealth**

In September of 2017, the Health Resources and Services Administration (HRSA) of the U.S. Department of Health and Human Services defined telehealth as: “the use of electronic information and telecommunications technologies to support and promote long-distance clinical health care, patient and professional health-related education, public health and health administration. Technologies include videoconferencing, the internet, store-and-forward imaging, streaming media, and terrestrial and wireless communications.”11

Telehealth technology can be either synchronous (in real-time, as with electronic fetal monitoring) or asynchronous, a/k/a “store-and-forward” (not concurrent, as with radiology films/scans). Below are examples of telehealth technology.

**Remote Monitoring Technology**

This modality of telehealth involves the collection of a patient’s personal health and medical data via electronic communication technologies. Patients can be monitored in non-clinical environments as well as in clinical ones. Once collected, the data are then transmitted to providers at another location. Remote monitoring is a form of telehealth that can be either synchronous or asynchronous. It can be used for conditions requiring immediate treatment or to monitor chronic conditions over time.12

**Wearable Devices/mHealth**

There are many wearable devices at present and they continue to be developed and improved. These devices can monitor patients outside an acute care or long term care setting. Such monitoring has the potential to markedly reduce health care costs. The future is exciting, as these devices can help not only with real-time monitoring, but also with prevention and early diagnosis. They can help patients remember to take medications and can detect non-adherence. They can serve as medical alarms when patients have an event putting them at risk. Commercial products such as Fitbits and smartphones can also be used track health and wellness.13

**Data Storage and Review**

This component of telehealth has been utilized for some time. Teleradiology is one of the earliest, and to date most common, uses. It is also called store-and-forward telehealth and is the collection of clinical information in various formats. These include videos; images; radiologic
scans, films and studies; sound files; laboratory reports and other medical records. It facilitates second opinions and, since its use is asynchronous, it is more convenient to both practitioners’ and patients’ schedules. This technology is used by many physician specialties such as radiology and also dermatology and ophthalmology, among others.14

Communication/Education

Patient and family education and communication can be greatly facilitated using software apps and online portals. Information to promote health and communication with health care professionals is available on demand.

Telemedicine (in real-time care delivery)

This component of telehealth is the “classic telemedicine” patient-provider encounter and the primary focus of this article. It is a live, two-way interaction between a provider and a patient in real-time using audiovisual equipment. It is performed using audio-visual equipment and the patient’s phone, tablet or computer. It can be done in a dedicated kiosk, such as often occurs in a commercial pharmacy setting. It can also involve video monitoring of the patient as in Tele-ICU monitoring, for example. The audio-visual technology used for these encounters has improved greatly in recent years.

CMS defines telemedicine as:

“A two-way, real-time interactive communication between a patient and a physician or practitioner at a distant site through telecommunications equipment that includes, at a minimum, audio and visual equipment.”15

Telemedicine Improves Care/Reduces Costs

Video visits with primary care providers offer access, convenience and speed to patients. They promote care in the lowest cost, often most appropriate setting. This form of telemedicine can prevent over-utilization in the form of reduced visits to physician offices, urgent care centers, and the emergency department; it can also avoid long waits for primary care. The telemedicine encounter typically costs appreciably less than office and urgent care visits and far less than ED visits.16 The biggest savings of all arise when because of distance care, admission to a hospital can be avoided.

Reimbursement is the Key

While there has been rapid adoption of many of the various components of telehealth and telemedicine, the key to future growth is reimbursement, especially by CMS. Commercial payers and employers have perceived the advantages of telemedicine and telehealth, and this has led to much greater acceptance in recent years of telemedicine and telehealth for reimbursement.17 Most major commercial health insurers are now offering various types of telehealth benefits.

A full discussion of reimbursement for distance care is beyond the scope of this piece. Until very recently, however, Medicare reimbursement has been limited to paying for only certain services, and only for beneficiaries who live in underserved or rural areas and who, at the time of care, were in health care facilities.18 Under its current leadership, however, CMS has embraced new codes for telehealth reimbursement. Two examples in 2019 are payment by CMS for care by telehealth methodologies for stroke and dialysis patients.19 CMS has also authorized reimbursement for some services rendered to beneficiaries in their homes, including patients undergoing home dialysis.

Regulatory and Statutory Issues

Licensure

Licensure is the primary mechanism states use to regulate the practice of medicine. They tend to guard their sovereignty jealously. States do not wish to cede this authority to the Federal government. That’s understandable, but it has created problems for professionals seeking to offer telemedicine services.

In traditional in-person care, of course, the physician and the patient are present together at a given location. A defining characteristic of telemedicine, however, is that the doctor is in one location; the patient, in another. Those locations could be in the same state, the same town, or even the same building, but they might be in different states or countries. One party could be here on
earth and the other in outer space. In every American jurisdiction that expressly answers the question, if the two participants are in different jurisdictions, the law (statute or regulation) provides that the care occurs at the patient’s location.20 In no jurisdiction, however, in any reported case, has any state’s highest court addressed the issue. In a few jurisdictions, the law is silent on where the care is provided in such circumstances. One of us has argued that, where the law is silent, one could take the position that the care is rendered at the provider’s location.21

Why does the question matter? Because the doctor must be licensed where the care occurs. If that were the physician’s own jurisdiction, he would already be licensed there, presumably, and would have no need for licensure elsewhere. Were the Board to make inquiry, the investigation and any potential formal or informal hearing would be in the doctor’s state. If, however, the care occurs at the patient’s out-of-state location, the physician needs to hold a license adequate under the laws of that state to care for its patients from afar, to submit to the jurisdiction of that state’s Board, and to be prepared to travel there if need be to defend himself before a hearing panel.

Despite the fact that in some places the law offers no express answer, the wiser course, and the only one we can recommend, is to assume that where the law is silent it would conclude that care occurs where the patient is and that, therefore, it behooves the provider to maintain licensure in the patient’s jurisdiction. The safest course for a doctor who proposes to care for patients in multiple jurisdictions, then, is to obtain and maintain licensure in each. The associated hassles are not trivial: each state charges a fee for licensure renewal, which will likely fall due on different dates; each has its own CME and documentation requirements; usually, each conducts hearings at its headquarters and will likely require the licensee to appear there in person. It would be better to learn after the fact that this multiple-license approach entailed needless effort, however, than to learn that the physician was engaged in what the applicable Board may deem to be the unauthorized practice of medicine in the patient’s state.

Depending on the jurisdiction, there may be an exception obviating the need for multiple licenses. States may enter into reciprocating agreements, for example. The District of Columbia allows a physician licensed only in Maryland to care for DC residents even though he lacks a DC license.22 Often, as in this example, the deal must be reciprocal: Maryland extends the same courtesy to DC physicians. Many states allow a doctor in another state to consult with one in-state even though the former is not licensed in the state. West Virginia, for example, allows practitioner-to-practitioner consultations, but for a single occasion only.23 In North Carolina, consultants without a NC license are allowed to care for patients on an “irregular basis.”24 Under licensure by endorsement, a state board accepts the license granted by another state with similar standards.25 Sometimes a state will allow a doctor in an adjoining state but within a short distance of the border to act as if he were licensed by the first state, or to provide virtual care across state lines in follow-up after a procedure such as a surgical operation. Some states issue special licenses / certificates related to the provision of telehealth services, allowing out-of-state providers holding such licenses to render services provided certain conditions are met, such as not opening an office in the state. Examples: Alabama, Louisiana, Minnesota, Montana, Nevada, New Mexico, Ohio, Tennessee, Texas, Wyoming. In many states, for a physician-to-physician communication, to which the patient is not a party, a license is not required. Sometimes this is very limited: Michigan allows consultation by an out-of-state physician only in “exceptional circumstances” (a term that does not appear to be defined).

Rhode Island offers a general consultation exception, but it appears that out-of-state physicians must obtain a Rhode Island license before providing telemedicine services in the state (even if they are just providing consultation). Other exceptions include medical emergencies and disasters, follow-up care, and free “curbside” consults.

In recent years, states have developed a compact, a kind of interstate contract, under which a physician licensed in one signatory state may shoulder a lighter administrative burden when he seeks licensure in another signatory state. Under the Interstate Medical Licensure Compact (“IMLC”)26, the physician must still become licensed in the second state and must still pay the fees associated with doing so. He becomes subject to the jurisdiction of the Board of Medicine in the second state. But in providing the documentation demanded by State #2, the Compact furnishes a mechanism that obviates the need to re-assemble transcripts, letters, diplomas, board certificates,
etc.; once these are gathered the first time the Compact enables them to be provided wherever needed thereafter. Psychologists and physical therapists have more-or-less analogous arrangements. The nurses have a far more sweeping Compact than do the doctors; theirs provides for recognition by one signatory state of a licensed issued by another signatory state.27

Credentialing and Privileging

Credentialing is the process health care organizations use to obtain, verify, assess and validate physicians’ experience and qualifications. Privileging is the process organizations use, after review of credentials, to grant authorization for a practitioner to provide a specific scope of patient care services. For many years, credentialing and privileging requirements hampered the growth of telemedicine, because the specialist at the academic center, for example, had to submit to the credentialing process at the community hospital where he was asked to consult from afar. This process was tedious and resource-intensive, especially for small rural hospitals under serious budgetary constraints.

In 2011, however, Medicare’s Conditions of Participation were changed to simplify the process significantly. Now, if certain requirements are met, the hospital receiving telehealth services may rely on the privileging and credentialing decisions of the hospital providing them. To engage in “credentialing by proxy,” the hospitals must have a written agreement that satisfies an array of criteria.28 The agreement must contain provisions requiring the distant-site hospital to use a credentialing and privileging process that meets or exceeds hospitals’ Medicare standards.29 The distant-site hospital must provide a list of telemedicine physicians and practitioners privileged there and their current privileges at the distant-site hospital to the hospital or CAH. The hospital must review the services provided to its patients by telemedicine physicians and practitioners covered by the agreement and must provide written feedback to the distant-site hospital addressing at least any adverse events or complaints that relate to the hospital or entity’s telemedicine services. The governing board of the distant site hospital must satisfy specified requirements.30 Satisfying all these requirements can be onerous, but this is still preferable to the old approach.

Depending on which jurisdiction’s law controls, harm caused by a failure to perform the credentialing and privileging functions for telemedicine services could give rise to a corporate negligence claim that might be difficult to overcome, particularly for a hospital or health care system. Failure to do so also may lead to allegations of the unauthorized practice of medicine, which can result in criminal fines, imprisonment, administrative penalties, and licensure suspension or revocation, with the attendant National Practitioner Data Bank implications. Other risks include payment denials, loss of liability insurance, and Conditions of Participation violations. Thus, those wishing to credential by proxy must do so mindful of the requirements and of the consequences of violations. The practice is nevertheless a significant advance, and reduces the administrative burdens associated with institutional distance care consults.

Privacy Issues

Apart, possibly, from financial data, few types of information are more sensitive to most of us than our health data. One’s medical record may document such matters as alcohol or substance abuse, mental illnesses, sexual abuse or sexually transmitted diseases, abortions, child or elder abuse, etc. Highly personal matters all. The law therefore goes to some lengths to protect information such as this from unauthorized dissemination. Its protections extend to virtual care just as they do to conventional, in-person care.

The 800-pound gorilla of American health records privacy law is HIPAA, Public Law 104-191, 110 Stat. 1936, as amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act. This statute was passed in large part to protect health insurance coverage for employees when they change or lose their jobs. Recognizing, however, that patients might worry about mishandling of their medical data, Congress also wrote HIPAA, and HHS enacted regulations, to provide protections for the privacy and security of what it calls “protected health information,” or PHI. Violations can result in fines and penalties, damaging publicity, and even, in egregious cases, criminal prosecution and imprisonment. Violations arise most often from human error, as when a healthcare professional leaves an unencrypted laptop on the train, for example. On the other hand, HIPAA applies
only to covered entities and to their business associates, and not, for example, to the makers of most medical apps. In an era, then, when not all health information is controlled by health care providers and insurers, HIPAA’s usefullness is circumscribed. Some argue that the law is outdated.

Long before 1996, when HIPAA was passed, every state in the Union had enacted statutes designed to protect health records as well. These vary in detail, complexity, and stringency, but they remain good law in the HIPAA era. Indeed, HIPAA itself provides that where, with respect to a given privacy issue, state law is more stringent than federal, state law controls. States such as California and New York are example of jurisdictions with particularly exacting requirements. And although under HIPAA there is no private right of action, under state law there often is.

Telemedicine Liability Issues

To date through mid-2019, there have been only a very small number of reported malpractice claims involving telemedicine in a real-time audio-visual encounter or in remote monitoring. Most of the cases filed in the last ten years or more involve teleradiology claims. In the very small remainder of claims, the issue of telemedicine is most always an incidental fact and not the true focus of the case.

Jurisdiction is potentially problematic in telemedicine cases if the encounter occurs across state lines. The courts of the state where the patient was at the time of the encounter will be the most likely place for litigation.

The issue of the appropriate standard of care for telemedicine is evolving. Plaintiffs will argue that that the standard of care in using telemedicine technology is the same as it is when a physical examination is conducted in person. Some state statutes or regulations, in fact, explicitly so provide. There is no case law to date on this point.

Corporate negligence is potentially a major area of exposure. Not credentialing providers, or doing so carelessly, or failing to see that they have the appropriate licenses and credentials to render telemedicine professional services will create hurdles in the defense of any case.

Depending on the rules of evidence in the relevant court, plaintiffs are apt to invoked state-specific statutes, medical board regulations, American Telemedicine Association guidelines, and specialty-specific guidelines promulgated by specialty societies such as the American College of Emergency Physicians (ACEP) or the American Psychiatric Association (APA) and many others, to attempt to establish the standard of care. The American Society for Healthcare Risk Management (ASHRM), in its “Telemedicine: Risk Management Considerations,” points to the Federation of State Medical Boards (FSMB) Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine as not only providing guidance from a risk management perspective, but also representing another form of voluntary guidelines that state medical boards may have adopted. Defendants often take the position that such documentary evidence ought not be used in attacks on defendants. Providers, however, should not merely assume that such arguments will carry the day. In preparing guidelines and the like, then, assuming they feel compelled to do so in the first place, providers should draft their documents with the expectation that their adversaries will try with might and main to use the documents against their drafters and their colleagues.

Telemedicine Claims Scenarios

As noted, telemedicine-related claims have been very few to date. If claims related to teleradiology or the use of remote electronic fetal monitoring are omitted, we are left with only a very few cases to study and learn from. Why is this so?

The numbers of telemedicine encounters to date, while increasing, have remained relatively low. This volume is projected to expand dramatically in the years ahead. Many of the encounters outside teleradiology have been in primary care scenarios where the conditions seen by the physician are mostly benign. But this is changing with rapid adoption of telemedicine technology in many specialties, as for example, to help treat psychiatric patients and stroke patients in remote locations. In the nature of things, broader utilization will, over time, engender more claims.

Informal polling of medical professional liability insurance carriers over the last few years revealed these actual, but minimally described, claims scenarios:
• Incorrect interpretations of images from a home setting (radiology)
• Miscommunication of the timeline for a “stat” reading of a (radiology) film from a home setting
• Failure to communicate presenting symptoms to a remote examining neuro-radiologist and allegedly resulting failure to diagnose a spinal abscess
• Failed telepsychiatry examination communications
• Incorrect diagnosis of a bacterial meningitis from a patient seen in a kiosk in a retail setting
• Suspected stroke incorrectly diagnosed by a telestroke consult
• Failure to adequately monitor remotely and assess an ICU patient for blood loss and hypotension, allegedly resulting in severe brain damage; failure to summon an intensivist for a more thorough bedside examination
• Telemedicine exam should have been performed in-person rather than by video

Telemedicine: Managing the Risk

Despite the paucity of claims to date, the potential for malpractice liability exists as the use of telemedicine expands rapidly. Perhaps the most important actions to be taken to prevent malpractice claims are to obtain good legal advice that thoroughly reviews all applicable state and federal laws and regulations, especially those of state medical board. Telemedicine-specific guidelines promulgated by accrediting organizations, such as the Joint Commission, should also be reviewed, even if only because of their likely use as foundations for arguments by plaintiff’s counsel.

Physician extenders must practice within their state’s licensure laws and defined scope. Credentialing of all providers for their competency and verification of licensure consistent with all state laws and regulations are essential. Staff training and clear definition of roles and documentation for a telemedicine encounter will reduce potential liability. Many organizations have internal telemedicine encounter protocols. These may offer some insights, but providers must remember they are highly likely to also offer ammunition to plaintiffs’ attorneys. Many medical specialties have created telemedicine-specific guidelines; these can be considered if an entity insists on creating practice or facility protocols.

As mentioned above, ASHRM (the American Society for Health Care Risk Management) has published an excellent, comprehensive monograph on managing telemedicine risk. The document is titled “Telemedicine: Risk Management Considerations” and was published in 2018.

In general, providers should generally not be the very earliest adopters of some new technological advance, but neither should they be the last to sign on. They should build in redundancy and secure good IT support for their distance care services, and should not permit midlevels (NPs and PAs), no matter how talented, to exceed the scopes of their licenses. Providers should educate patients about the limitations of telemedicine and remain astute to decline to use the technology to care for patients whose symptoms suggest that in-person evaluation is indicated. Even where no specific authority compels it, providers offering distance care should obtain and document consent. They should also be cautious in describing the benefits of telemedicine, allowing enthusiasm to overtake reality. Plaintiffs will not hesitate to base contract or warranty claims on overly bullish descriptions even though their authors never intended to make any promises. At each encounter, providers must identify all in attendance and verify their physical location. Providers using telemedicine to care for children should insist that parent or guardian be present, except in cases (adolescents with sexual or substance use problems, for example) where they may not lawfully do so.

Underwriting Telemedicine: Medical Professional Liability

Owing to telemedicine’s explosive growth underwriting medical professional liability insurance for patient-provider telemedicine and the wide range of telehealth technologies encounters is becoming more common. Some insurers have specific policies developed for this service.

But the exposures for telemedicine go beyond medical professional liability, and thus buyers, brokers and underwriters should recognize other significant related
and insurable risks and tailor insurance coverages appropriately. These might include general liability, cyber liability, product liability, and tech errors and omissions liability, depending on the nature of the telemedicine/telehealth products and services.

Here are a few key considerations for insuring or placing coverage for telemedicine:

• Is there intrastate or interstate exposure? How rapidly is the entity expanding across state lines?

• Numbers of patient encounters in the past/projected and numbers by location/territory?

• Is there any international exposure? For example, physicians in a foreign country reading studies or seeing patients through video visits.

• Verification of provider compliance with all applicable licensure laws: statutory or regulatory.

• What portion of the provider’s practice is dedicated to distance care?

Conclusion

Telemedicine and telehealth are revolutionizing care delivery not just in the United States but across the globe. The demand for patient-provider video encounters is growing as is their sheer numbers. The technology can help address the shortage of primary care and specialist physicians and mental health professionals outside urban settings.

Telemedicine and telehealth can lower costs, especially by redirecting appropriate patient care from more costly settings, whether it is urgent care, emergency departments, the acute care hospital or a long term care settings to cheaper ones, thereby also increasing access and convenience for patients and families.

The number of tort claims to date is very low and this is likely a function of the relatively low numbers of patient encounters so far. It may also be attributable to the fact that providers are simply providing good, thoughtful care.

Telemedicine/telehealth risk is insurable, as its risks are manageable with attention to how insureds comply with state and federal laws and the customs of their peers, to licensure, and to the other issues considered here. There is great opportunity for the property/casualty insurance industry to grow premium and meet the needs of organizations and providers engaged in telemedicine and telehealth. This extends beyond medical professional liability to coverage for cyber risks, tech E&O, life sciences coverage, and potentially other areas as well.

ABOUT THE AUTHORS

PAUL A. GREVE JR., JD
RPLU
is Senior Director Healthcare Risk Solutions, Markel Assurance. Paul oversees Markel’s clinical risk management services and provides consulting to Markel insureds. Paul has twenty five years’ experience in the MPL insurance industry and previously held risk management and legal positions at major Ohio hospitals. He can be reached at paul.greve@markel.com

JOSEPH P. (“JOE”) MCMENAMIN, MD, JD
is a physician-attorney and the principal at McMenamin Law Offices, PLLC, a healthcare boutique concentrating on the law of digital health. He has many years’ experience in defending health care providers and pharmaceutical, medical device, and biotech companies against a variety of allegations in state and federal court. He can be reached at mcmenamin@medicalawfirm.com

PAUL A. GREVE JR., JD
RPLU
is Senior Director Healthcare Risk Solutions, Markel Assurance. Paul oversees Markel’s clinical risk management services and provides consulting to Markel insureds. Paul has twenty five years’ experience in the MPL insurance industry and previously held risk management and legal positions at major Ohio hospitals. He can be reached at paul.greve@markel.com

JOSEPH P. (“JOE”) MCMENAMIN, MD, JD
is a physician-attorney and the principal at McMenamin Law Offices, PLLC, a healthcare boutique concentrating on the law of digital health. He has many years’ experience in defending health care providers and pharmaceutical, medical device, and biotech companies against a variety of allegations in state and federal court. He can be reached at mcmenamin@medicalawfirm.com
End Notes


23. WV Code 30-3-12(d)(8).


27. https://www.ncsbn.org/nlc.htm

28. 42 C.F.R. 482.12(a)(8), (a)(9).

29. 42 CFR §482.12(a) and 42 CFR §482.22(a).

30. (42 CFR §482.12(a)(1) -(a)(7)).


32. 45 CFR §160.203(b).
Join the PLUS Foundation and colleagues for this long-standing benefit prior to the start of the PLUS Cyber and D&O Symposia. Each year, Strikes for Charity participants get together for a fun evening of networking, bowling and raising money for the PLUS Foundation.

Purchase a lane, become a sponsor or join us for networking – it’s an evening worth your time with fabulous food and a hosted bar!! The event fills fast, so get your spot locked-in today!

For more information – plusfoundation.org/strikes-for-charity
2019 PLUS CONFERENCE

EVENT RECAP
The PLUS Conference is the ultimate experience to learn about the professional liability industry and connect many of the top leaders and experts. This Conference continues to be the leading event in the industry and this year was no different.
“PLUS PROVIDES GREAT INSIGHTS ON A VARIETY OF TOPICS FROM LEADERS IN THE FIELD.”

“IT’S A GREAT OPPORTUNITY TO BE EXPOSED TO COMING INSURANCE TRENDS IN THE MARKETPLACE. THOSE TRENDS USUALLY HAVE AN IMPACT ON THE CANADIAN MARKETPLACE AS WELL.”
“A GREAT WAY TO PLACE THE NAME WITH THE FACE OF THOSE YOU DO BUSINESS WITH. RELATIONSHIP BUILDING!”

“EXCELLENT QUALITY PROGRAMING -- THE BEST!”
If you missed this year’s Conference, you don’t want to miss the 2020 Conference!

Join us in Orlando, Florida on November 9-11 at the Ritz Carlton and JW Marriott.
NEW REGULATION BEST INTEREST BECOMES EFFECTIVE FOR BROKER DEALERS

BY: BARRY R. TEMKIN AND MELISSA TARENTINO

On June 5, 2019, the Securities and Exchange Commission (the “SEC”) voted to adopt a package of rules and interpretations “designed to enhance the quality and transparency of retail investors’ relationships with investment advisers and broker-dealers.” Regulation Best Interest (“Reg. BI”) went into effect on September 10, 2019, with a compliance date of June 30, 2020.

The SEC was mandated by the Dodd Frank Wall Street Reform and Consumer Protection and Act of 2010 to study the feasibility of adopting a fiduciary standard for registered securities representatives. Currently Registered Investment Advisers are held to a fiduciary standard by the SEC, whereas Registered Representatives are governed by a suitability standard implemented by the Financial Industry Regulatory Authority (FINRA), which issues their licenses. Investor advocates complained that
the dual standards would be confusing to customers, especially since many advisers are dually registered as both registered representatives and IARs. Meanwhile, the SEC bided its time, taking over nine years after Dodd Frank to promulgate its not-fiduciary but fiduciary-like standard. In the meantime, the Labor Department, under the Obama Administration, leapt into the absence left by the SEC, and promulgated its own, highly complex fiduciary regulations, which applied to recommendations by RRs in retirement accounts only. Apparently the DOL felt that two standards were not sufficient, and that it would be wise to have a third standard, only applicable to retirement savings. The DOL fiduciary standard was short-lived, as it was promptly struck down by the Fifth Circuit Court of Appeals as beyond the agency’s authority.

SEC Reg. BI is similar, but not identical to a fiduciary standard. As Michael Kitces writes, for broker-dealers, “the rule requires greater disclosures of their business practices, a requirement to take active steps to mitigate conflicts of interest and an outright ban on certain sales contests, quotas and similar problematic incentives.”

The regulation contains a General Obligation, which requires that broker-dealers “when making a recommendation of any securities transaction or investment strategy involving securities (including account recommendations) to a retail customer... act in the best interest of the retail customer... act in the best interest of the retail customer at the time the recommendation is made, without placing the financial or other interest of the broker, dealer, or natural person who is an associated person of a broker or dealer making the recommendation ahead of the interest of the retail customer.” In order to satisfy the General Obligation, a broker dealer must satisfy the following four component obligations: (1) the Disclosure Obligation, (2) the Care Obligation, (3) the Conflict of Interest Obligation, and (4) the Compliance Obligation. Thus, “whether a broker-dealer has acted in the retail customer’s best interest will turn on an objective assessment of the facts and circumstances of whether the specific components of Regulation Best Interest are satisfied at the time that the recommendation is made.” Note that the regulation applies, by its terms, to “the time the recommendation is made,” and does not impose an ongoing obligation to monitor the customer’s accounts.

1. DISCLOSURE OBLIGATION

The Disclosure Obligation requires that a broker-dealer provide “in writing, full and fair disclosure of: (A) All material facts relating to the scope and terms of the relationship with the retail customer...[and] (B) All material facts relating to conflicts of interest that are associated with the recommendation.” Relative to the “material facts relating to the scope and terms of the relationship,” a broker-dealer must disclose that (i) the firm is acting as a broker-dealer, not an investment adviser; (ii) the “material fees and costs that apply to the retail customer’s transactions, holdings, and accounts;” and (iii) “the type and scope of services provided to the retail customer, including any material limitations on the securities or investment strategies involving securities that may be recommended to the retail customer.” The phrase “material facts” and “material fees and costs” are interpreted with the standard of materiality set forth in Basic, Inc. v. Levinson. Moreover, under Reg BI, broker-dealers, like RIAs, are obligated to complete a new Form CRS (Customer/Client Relationship Summary) prior to or contemporaneously with the adviser’s recommendation, explaining the types of client/customer relationships and the services the firm offers, the fees, costs, conflicts of interest and required standard of conduct associated with those relationships and services, and the firm’s reportable legal or disciplinary history.

2. CARE OBLIGATION

The Care Obligation has a three-pronged suitability requirement. The adviser must first determine that the product is good for someone. Then the adviser must decide that the recommended security is good for the particular individual retail investor to whom she makes the recommendation. Third, the amount recommended must be reasonable for the investor; i.e., the customer must not be overly concentrated in that position. The Care Obligation thus builds upon, but goes beyond, FINRA’s existing suitability obligation by mandating that a recommendation be in a retail customer’s “best interest” and that the broker-dealer must not place its own interest above that of the customer’s. Furthermore, the SEC has noted that broker-dealers should consider reasonably available alternatives when assessing whether they have a
“reasonable basis” that a particular recommendation is in the customer’s best interest.12

**3. CONFLICT OF INTEREST OBLIGATION**

The Conflict of Interest Obligation requires a broker-dealer to establish, maintain and enforce written policies and procedures reasonably designed to:

(A) Identify and at a minimum disclose, in accordance with [the Disclosure Obligation], or eliminate, all conflicts of interest associated with such recommendations;

(B) Identify and mitigate all conflicts of interest associated with such recommendations that create an incentive for a natural person who is an associated person of a broker dealer to place the interest of the [broker-dealer] ahead of the interest of the retail customer;

(C) (1) Identify and disclose any material limitations placed on the securities or investment strategies involving securities that may be recommended to a retail customer and any conflicts of interest associated with such limitations, in accordance with [the Disclosure Obligation], and

(2) Prevent such limitations and associated conflicts of interest from causing [the broker-dealer] to make recommendations that place the interest of [the broker-dealer] ahead of the interest of the retail customer;13

In addition, Reg BI prohibits “sales contests, sales quotas bonuses and non-cash compensation that are based on sales of specific securities or specific types of securities within a limited period of time.” Reg. BI defines a “conflict of interest” as “an interest that might incline [the broker-dealer] – consciously or unconsciously – to make a recommendation that is not disinterested.”14

Furthermore, because broker-dealers are required to disclose conflicts of interest in accordance with the Disclosure Obligation, the SEC stated “where a broker-dealer cannot fully and fairly disclose a conflict of interest in accordance with the Disclosure Obligation, the broker-dealer should eliminate the conflict or adequately mitigate (i.e., reduce) the conflict such that full and fair disclosure…is possible.”15 The SEC provided a non-exhaustive list of incentives paid to an associated person that would need to be addressed under the Conflict of Interest Obligation, as well as potential methods to mitigate such conflicts.16

**4. COMPLIANCE OBLIGATION**

Under the Compliance Obligation, a broker-dealer must also establish, maintain, and enforce “written policies and procedures reasonably designed to achieve compliance with Regulation Best Interest.”17 This newly-added section “creates an affirmative obligation under the Exchange Act with respect to [Reg. BI] as a whole, while providing sufficient flexibility to allow broker-dealers to establish compliance policies and procedures that accommodate a broad range of business models.”18 The Compliance Obligation operates to “ensure that broker-dealers have strong systems of control in place to prevent violations of [Reg. BI].”19 The SEC also noted that “a reasonably designed compliance program generally would also include: Controls; remediation of non-compliance; training; and periodic review and testing,” but that an individual firm’s program should be “reasonably designed to address and be proportionate to the size, scope and risks associated with the operations of the firm and the types of business in which the firm engages.”20

**CONCLUSION**

The SEC has provided a compliance date of June 30, 2020 in order to provide “adequate notice and opportunity for broker-dealers to comply with [Reg. BI].” The new regulations require broker-dealers to eschew sales contests which encourage sales of particular products (as notoriously lampooned in the movie “Boiler Room.”) It should be noted that the SEC regs require that the recommendations be in the investors’ best interest at the time of the recommendation, and do not require continuing monitoring of existing positions.

Reprinted with permission from the “9/25 edition of the “New York Law Journal”© 2019 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited, contact 877-257-3382 or reprints@alm.com.


5 Reg BI at n.16.

6 Id. at 33,491.

7 Id.

8 485 U.S. 224 (1988) (a fact is material if “there is a substantial likelihood that a reasonable shareholder would consider it important”).


10 Reg. BI at 33,491.


12 Reg BI at 33,381.

13 Id. at 33,491.

14 Id. at 33,491.

15 Id. at 33,388-89.

16 Id. at 33,391-92.

17 Id. at 33,491.

18 Id. at 33,397.

19 Id.

20 Id. at 33,397-98.
You could have a surprise trial in less than a week pursuant to a little-known statute in California. Specifically, California Corporations Code § 709(b) allows any person who claims to have been denied the right to vote in a board member election to challenge the directors’ position on a California company. Specifically, the California statute requires the court to determine the validity of any election or appointment of any director of a corporation through an evidentiary hearing within five days. Of course, this provide an enormous advantage to any would-be plaintiff seeking to unseat a director of a California domestic corporation or foreign corporation if the election was held in California.

Court has Broad Discretion under Section 709

Section 709 is not limited to voting rights. The court has broad discretion to consider all matters necessary to determine the validity of a contested election. The statute creates an equitable cause of action which allows the Court to rule upon issues or causes of action related to an election. This includes breach of fiduciary duty, fraud, conflict of interest, legality of contracts, or whether a person is a shareholder. The court could rule upon these complex issues on a summary basis before any discovery has even taken place.

For example, in *Morrical v. Rogers*, the California Court of Appeals confirmed the trial court’s ability to summarily decide breach of fiduciary duty and conflict of interest claims during the 709 hearing. In this case, the shareholder asked the court...
to invalidate the previous election of the board of directors and to set aside all actions taken by those directors on the basis that the directors had material financial interests which created a conflict. The Court stated that “they [found] no basis to infer an unwritten limitation on the scope of an action under Section 709 where the Legislature has not expressly provided such a limitation.” Therefore, the court reasoned that the trial court had discretion to decide the related issues of the breach of fiduciary duty and conflict of interests. While the court would eventually remand the case back to the trial court because the majority shareholders were indispensable parties and not part of the action, the court’s reasoning still stands. Courts have wide discretion to decide complex, collateral issues during an immediate Section 709 trial.

Who Can Demand a Section 709 Trial

California Corporations Code § 709 is not limited to shareholders of a corporation. Under subsection (a), “Upon the filing of an action therefor by any shareholder or by any person who claims to have been denied the right to vote….” Any person who claims to have been denied the right to vote at an election or appointment of a director has standing to demand a Section 709 trial. This would include investors who had entered into a subscription agreement, those who entered into agreements to take shares but have not yet been issued the shares, corporate trustees, or even those claiming to be shareholders which the corporation disputes.

What Can You Do?

There are two things which can assist in navigating and preparing for a Section 709 hearing. First, the corporation should communicate and prepare for a potential Section 709 hearing immediately upon receiving notice that an election may be challenged. This includes gathering and organizing the necessary documents to support the election and determining on what grounds the election might be challenged. For example, a shareholder may challenge the validity or voting rights of a preferred stockholders. In this instance, the corporation would not only gather all the documents relating to the election, but also documents relating to the issuance of the preferred shares (e.g. the bylaws, articles of incorporation, minutes of the Board of Directors meetings, etc.) Then if the shareholder files a complaint and demands an immediate Section 709 hearing, almost all of the documents will be ready to discuss with the attorney. This will maximize the short amount of time you have to prepare for the expedited trial.

Second, the corporation can request the Section 709 trial be set for more than five days under a showing of good cause. Good cause might include if you can show limited discovery might be necessary or if your counsel is unavailable in the next five days. Finally, if the related issues are extremely complex, one could argue that the scope of Section 709 trial be limited in scope as to not deprive the corporation or individuals of their constitutional due process. While courts have ruled that due process was not violated in the past, some courts have left the door open that if the issues were complex enough it would be possible for a violation of due process to occur. While there is no guarantee the court will find good cause and fix the hearing date more than five days, you will have a much better chance in obtaining a slight extension.

ABOUT THE AUTHORS

JOHNNY ANTWILER is a senior associate of O’Hagan Meyer in its Los Angeles and Orange County offices. His practice focuses on securities litigation, financial services litigation, directors and officers (D&O) liability defense, white collar defense, professional liability, and commercial litigation. Johnny has extensive experience representing broker-dealers, financial professionals, directors and officers, and corporations in both federal and state court, FINRA arbitrations, and investigations and actions brought by the U.S. Securities and Exchange Commission.

SAM Y. EDGERTON, III is a partner of O’Hagan Meyer in its Los Angeles and Orange County offices. He is the Co-Chair of the firm’s Financial Services and Securities Group. Sam is a trial attorney with extensive litigation experience in federal and state federal courts, as well as FINRA arbitration matters. A former prosecutor, Sam has extensive experience in white collar defense in government cases both civil and criminal where he represents officers and directors of public and private companies. He also represents a myriad of licensed professionals such as financial planners, insurance agents, accounting professionals and lawyers.
End Notes

3 Id. at 457.
4 Id. at 460.
Tremendous thanks to our 2019 donors for driving our mission of reflecting the generosity of the professional liability insurance community. Thanks to you we are able to support charities, engage hundreds of volunteers and provide quality programs and scholarships across the U.S. and Canada.

PLATINUM DONORS

GOLD DONORS

SILVER DONORS

Nancy Adams
AIG
Allianz Global Corporate & Specialty
ARC Excess & Surplus
Bailey Cavalieri LLC
Berkley Professional Liability, a Berkley Company
Dykema Gossett
Chasnoff Mungia
GenRe

Markel
Nationwide
Norton Rose Fullbright US LLP
Old Republic
OneBeacon Professional Insurance
PLAN
Wilson Elser
XL Catlin
Zurich North America

BRONZE DONORS

Axis Insurance Services LLC
BatesCarey LLP
Business Risk Partners
CRC
Doyle, Restrepo, Harvin & Robbins
Great American Insurance Group
Halper Keating Foundation
Jeff Cowhey
Robert Crocitto

Lynn Kimmel Johnson
Jeff Klenk
Maria Treglia
Mendes & Mount
Neher Family
O’Hagan Meyer
Susan Rivera
RLI Insurance Company
DON’T LET THE CYBER LIABILITY INDUSTRY MOVE FASTER THAN YOU.

GET ALL YOU NEED TO KNOW AT THE 2020 CYBER SYMPOSIUM

Feb. 25-26
New York, NY
Marriott Marquis