Telemedicine Law and Liability: 2015

By Joseph P. McMeniman & Paul A. Greve, Jr., JD, RPLU

Telemedicine has been growing exponentially in recent years and will continue to do so over the next decade. Telemedicine has the potential to improve care and reduce cost, goals fully consistent with the aims of health care reform. Indeed it is mentioned in the Affordable Care Act for just that purpose.

Congressman Mike Thompson, D-California, introduced the Medicare Health Parity Act of 2015 on July 7, a bill that would expand coverage for telemedicine for Medicare beneficiaries. Thompson and his three co-sponsors said the bill would place Medicare “on the path toward parity with in-person healthcare visits.” Thompson also said, “Both patients and providers want telehealth for two simple reasons—it saves money and saves lives.”

Telemedicine raises many legal issues, particularly from a regulatory and liability perspective. It is important for underwriters, agents, brokers, health care lawyers and risk managers to understand the legal implications of telemedicine. This article is a brief overview of some of those issues.

Telemedicine Defined

There has never been consensus on the definition of the term “telemedicine.” The term “telehealth” is sometimes used as well and may comprise non-clinical services. The terms may or may not be interchangeable depending on the context, but the American Telemedicine Association does consider them to be synonyms and as “encompassing a wide definition of remote health care.”

In 2014, the AMA issued a report on Coverage and Payment for Telemedicine. In it they described three different, broad types of telemedicine technologies: remote monitoring technology, store-and-forward technology, and (real-time) interactive services. The last category is the one most often considered as best fitting the definition of telemedicine.

Store-and-forward technology allows for “asynchronous” communication in which images or data are stored and sent as files to providers who then respond with an assessment.

Types of Telemedicine Services

Primary care/specialist consultation

These consultations serve diagnostic purposes. They often involve live interactive video. They can also entail transmission of patient vital signs, old records, video clips, and especially diagnostic images. Teleradiology has burgeoned over the last decade. Especially for interactive video, the challenge is for providers to judge when the patient needs to be seen in person rather than over a screen.

Remote patient monitoring

This category of telemedicine uses technologies to gather data for interpretation and transmit them to a remote diagnostic testing facility (“RDTF”) or to another entity such as a clinic, hospital, physician’s office, or home health agency. Examples may include such information as vital signs, electrocardiograms, blood tests, and others. Although generally healthcare professionals interpret this information, patients can themselves use sensors to measure their own personal indicators of disease at home as well.

Telemedicine Liability

To date there has been an almost infinitesimally small number of reported malpractice claims involving telemedicine. Even in those cases filed, telemedicine may not be the primary focus of the plaintiff’s lawyer. Often, it is merely part of a fact pattern.

The defense of telemedicine malpractice claims can be complex for many reasons. One is simply that the dearth of...
Correcting Incorrect Opinions about Omnicare

By Douglas W. Greene & Claire Loebz Davis

In Omnicare, Inc. v. Laborers Dist. Council Const. Industry Pension Fund, the Supreme Court held that a statement of opinion is only false if the speaker does not genuinely believe it, or if – as with any other statement – it omits facts that make it misleading. The Court’s ruling on what is necessary for an opinion to be false establishes a uniform standard that resolved two decades of confusing and conflicting case law, which often resulted in meritless securities cases surviving dismissal motions. And the Court’s ruling regarding how an opinion may be misleading requires courts to judge the fairness of challenged statements within a broad factual context, eliminating the short-shift that many courts have given misleading-statement analysis.

These are tremendous improvements in the law, and will help defendants win more cases, not only under Section 11, the statute at issue in Omnicare, but also under Section 10(b), since Omnicare’s holding applies to the “false or misleading statement” element common to both statutes. Yet we continue to see extensive commentary from defense lawyers saying that the ruling expanded the basis for defendants’ liability. That is simply wrong. Indeed, Omnicare has the potential to be the most helpful Supreme Court decision for defendants since Tellabs, if we in the defense bar use it correctly.

**Pre-Omnicare Law Governing Statements of Opinion Was Muddled**

To correctly understand Omnicare, it is critical to appreciate the messiness of the law on statements of opinion before the decision.

The Supreme Court first addressed the issue of what makes a statement of opinion false in Virginia Bankshares v. Sandberg. Virginia Bankshares held that an opinion may be actionable as a false statement of “fact,” only if it is a “misstatement of the psychological fact of the speaker’s belief in what he says.” This makes sense. If it is raining, but Joe says that the weather is “nice,” his statement of opinion is true if he genuinely believes it – if Joe genuinely likes rainy weather. It doesn’t matter if most other people wouldn’t think so.

Virginia Bankshares did not catch on. We think there are two main reasons. First, the decision is convoluted, making it difficult to read and decipher. Many doubted that the Supreme Court actually meant to create a so-called “subjective falsity” standard, and many defendants and courts did not even cite the case when analyzing statements of opinion.

Second, the Virginia Bankshares subjective falsity standard only covered the “false” half of the “false or misleading statement” element – the fact of the speaker’s state of mind – and did not address the question of whether a “true” statement of opinion can omit facts that make the opinion misleading. In the example above, Joe’s opinion could be true, but is nonetheless misleading to a reasonable person, since most people do not regard rainy weather as “nice.” Courts thus struggled to figure out how to harmonize Virginia Bankshares with the “misleading” half of the element, especially as defendants argued that a lack of subjective falsity defeated all claims regarding statements of opinion. Understandably, courts did not believe this result was fair, because it would effectively immunize any statement of opinion from being “misleading.” We believe that this difficulty led courts to ignore or distinguish Virginia Bankshares, or to apply an alternative standard.

The most influential alternative standard was the disjunctive three-part test the Ninth Circuit established in 1989 in In re Apple Computer Sec. Litig. In Apple, the Ninth Circuit held that opinions are actionable if they (1) are not genuinely believed, (2) there is no reasonable basis for the belief, or (3) the speaker knows undisclosed facts that tend to seriously undermine the opinion. Although Apple was decided before Virginia Bankshares, the court held that it was not actually believed by the speaker. This likely is the source of the defense bar’s disappointment with Omnicare: they feel it is a step backward from the standard of law they hoped for an afterthought.

Even after the Ninth Circuit first applied Virginia Bankshares in 2009, in Rubke v. Capitol Bancorp Ltd., it didn’t expressly overrule the incompatible Apple standard, and some courts, both inside and outside the Ninth Circuit, continued to refer to Apple. This tide began to turn in 2011, when the Second Circuit decided Fait v. Regions Fin. Corp., and joined the Ninth Circuit in correctly applying Virginia Bankshares. Based on Fait and Rubke, and a few other circuit court decisions, defendants began to argue that an opinion can only be false or misleading if it was not actually believed by the speaker. This likely is the source of the defense bar’s disappointment with Omnicare: they feel it is a step backward from the standard of law they hoped for an afterthought.

But that standard is not supported by either Virginia Bankshares or the relevant statutes. Section 11 and Section 10(b) specify that a “true” statement can be actionable if it is nonetheless misleading. As to statements of fact, it is accepted that a statement is misleading if the speaker omits facts that would cause a reasonable person to misunderstand the true state of affairs. Virginia Bankshares simply did not address the “misleading” portion of the standard for statements of opinion, and most of the cases that followed it sidestepped this complication. In Omnicare, the
Tibble v. Edison International: What Does It Mean for Fiduciaries and Their Insurers?

By Deborah S. Davidson & Kimberly M. Melvin

For the second year in a row, the Supreme Court decided an ERISA breach-of-fiduciary duty case involving the management of retirement plan investments and left open several issues for the lower courts—and plan fiduciaries—to sort out going forward. Last year it was *Fifth Third Bancorp v. Dudenhoefер*,¹ which eliminated the fiduciary-friendly “prudence presumption” that most courts had applied to investments in employer stock. This year it was *Tibble v. Edison International, et al.*, an excessive fees case.² In *Tibble*, the Court confirmed that an ERISA fiduciary has an ongoing duty to monitor plan investments, and held that ERISA’s six-year statute of limitations would not bar a claim challenging investments in a plan that had been selected more than six years before the alleged fiduciary breach. The Court left open, however, the specific parameters of the fiduciary duty to monitor investments and remanded the case for further proceedings.

**Backdrop to *Tibble***

*Tibble* is one of the “excessive fee” class action lawsuits filed in recent years against plan sponsors, fiduciaries and service providers of defined contribution retirement plans. Plaintiffs argue in these cases that the prudent investment standards of ERISA’s duty of prudence and loyalty by, among other things, investing in retail mutual funds instead of institutional class funds on the theory that the latter are cheaper; (4) offering united employer stock funds (under the theory that a unitized fund’s cash buffer and transaction fees deplete investment returns); (5) allowing service providers to retain “float” on plan investments; (6) selecting proprietary investment funds managed by an affiliate of the plan sponsor and/or fiduciaries rather than selecting allegedly lower-cost and better-performing funds from the marketplace; (7) paying asset-based service provider fees (e.g., recordkeeping); (8) failing to appropriately offset revenue sharing against the plan; and (9) allowing the plan’s fees to “subsidize” a service provider’s provision of non-plan services.

In some instances, the initial selection of the challenged investments or services occurred many years before the complaint was filed. Under ERISA, a plaintiff generally must bring a claim for fiduciary violations within no more than six years after “the date of the last action which constituted a part of the breach or violation,” in the absence of fraud or concealment.³ This led several courts, including the United States Courts of Appeal for the Fourth, Ninth and Eleventh Circuits, to dismiss excessive fee claims as time-barred when the plaintiffs could point to no change in circumstances establishing a new or distinct breach within the six-year limitations period.⁴ These courts also rejected the plaintiffs’ “continuing violation” theory that a new fiduciary breach occurred within the limitations period every time the fiduciaries failed to “correct” the original (time-barred) breach.⁵

**Tibble's Procedural History**

The *Tibble* plaintiffs filed suit against Edison International and several other defendants in August 2007, claiming that fiduciaries of Edison’s 401(k) plan breached their ERISA duties of prudence and loyalty by, among other things, investing in retail class mutual funds that charged high fees, when identical—but cheaper—institutional class funds were readily available.⁶ The district court granted summary judgment in favor of the plan fiduciaries on the majority of plaintiffs’ claims, and also ruled on “an independent basis” that ERISA’s limitations period barred recovery for claims arising out of investments that had been selected for the plan more than six years before the plaintiffs had filed suit.⁷ The court denied summary judgment with respect to six mutual funds.

Following a bench trial, the district court decided the plaintiffs’ remaining claims. The court ruled in favor of the plan fiduciaries with the exception of three funds that had been selected for the plan in 2002. With respect to those funds, the court ruled that the plan fiduciaries breached their duties of prudence and loyalty by selecting retail-class mutual funds without adequately investigating the availability of lower-cost institutional class versions of the same funds.⁸ The court awarded damages of $370,000.

On appeal, the Ninth Circuit agreed that offering mutual funds as plan investments was not a breach of ERISA’s duty of prudence and rejected a bright-line rule that only institutional-class mutual funds are prudent. The court also ruled that the plan fiduciaries did not breach any ERISA duties in including a unitized stock fund or a short-term investment fund as plan investments or through the plan’s revenue sharing practices.⁹

The Ninth Circuit also affirmed the district court’s rulings with respect to the statute of limitations for plan investments that had been selected more than six years before the plaintiffs had filed suit. Like the district court, the Ninth Circuit viewed the act of “designating an investment for inclusion” to start the six-year limitations period and found that “[c]haracterizing the mere continued offering of a plan option, without more, as a subsequent breach” would

---

¹ *Fifth Third Bancorp v. Dudenhoefer*
Q&A With PLUS Executive Director Robbie Thompson

New PLUS executive director Robbie Thompson hit the ground running, engaging with members and offering insight into PLUS operations via his First 100 Days Blog (check it out at http://plusblog.org/author/rthompsonplus/). He recently spoke with the editors of PLUS Journal about his vision for PLUS and associations, as well as his work experience prior to joining the PLUS team.

PLUS: Why did you choose to become the PLUS executive director?

Robbie: First, let me say how honored I am to have been given this opportunity. In a modest number of years by association standards, PLUS has clearly become a relevant, influential part of the Professional Liability industry. I truly appreciate the chance to come here and build on those past successes and utilize the association management experience I have gained in my other association management positions to help move PLUS forward.

PLUS: What did you do prior to joining PLUS?

Robbie: Prior to joining PLUS I was the President/CEO of the Credit Union Association of the Dakotas (CUAD). In that role I lead a dynamic team of association professionals whose primary mission was to help credit unions in North and South Dakota succeed. At CUAD we focused on legislative and regulatory advocacy, public relations and awareness, and education and professional development. I also had the opportunity to work at three other associations over my career in Minnesota and New Jersey, and through these experiences I have seen a lot of what works and what does not for associations. I hope these experiences can be invaluable to PLUS.

PLUS: What are some of your goals for your first 12 months with PLUS?

Robbie: The PLUS board of directors, previous boards, the previous executive director, and the staff at PLUS has already created a strong foundation to continue to be a forward looking association and my job is to continue to build on that. To do so I plan to do a lot of listening to members. I want to take every opportunity I can to hear what are members’ professional needs, what is happening to the industry and their thoughts on how PLUS can be even more relevant to them. I plan to use that knowledge to work to make PLUS more nimble and innovative. I hope over the next few months to move PLUS in a direction so that it can adapt quickly and even be in front of the rapidly changing demands of members and of the evolution of the industry. I also plan to work to encourage the organization to take a few chances and try some new things that will help PLUS build stronger emotional connections with members.

PLUS: What do you view as the biggest business challenge for associations in the coming years?

Robbie: I believe the association model is still the best model to bring people together and work collectively for an industry. Yet, it must adapt. Associations face tremendous competition, particularly for dues and education dollars from many different directions that did not exists years ago. This gives members a lot more options on how to spend their limited dues and education dollars. So associations needs to do more to remove layers of bureaucracy, utilize data more, specialize memberships to meet the individual needs of each member, and recognize that members must both feel connected to the association and feel that the association provides them with a real direct benefit.

PLUS: What do you see as the greatest opportunity for PLUS in the coming years?

Robbie: As I have the opportunity to visit with members over the coming months I expect those conversations to help me uncover additional opportunities for PLUS, but today the first opportunity is for PLUS to deepen its relationships with all of its members. Today PLUS has a lot of members who are passionate about their association and I think we can get even more people involved in and passionate about PLUS. Second, PLUS has tremendous opportunities to expand its global reach. More and more liability insurers are expanding their global markets and PLUS can be there along with them to help develop talent and further the knowledge of and the need for professional liability insurance in those areas. Third, PLUS can improve on telling its own story. It’s a good one, but I think members and potential members often really don’t know all that PLUS has to offer and all that it does. We need to celebrate our successes more, celebrate members’ successes more, and not be afraid to toot our own horn. And, I think PLUS is well positioned and has the type of membership that is welcome to exploring new ways to get education and new ways to obtain knowledge.

PLUS: What was something that surprised you about PLUS as you researched the organization?

Robbie: Maybe not so much during the search process, but during my first few weeks I was surprised by how deep the passion for the organization is by many of the members. Many members
have told me about how PLUS was instrumental in helping them build their career, making lifelong connections, building their business and expanding their knowledge. And it’s not just a “I like PLUS,” it is more of dare I say a love affair or at least a deep admiration. That certainly provides me motivation to continue that success, and work toward getting everyone in the industry to have that same feeling about PLUS.

PLUS: What should PLUS members know about you?

Robbie: Besides being short, bald, and needing to shed a few pounds you mean right? Honesty I am a pretty regular guy. I believe in hard work, trying to be the best at everything you do, being honest and taking care of your family. I would like members to know that I plan on being part of positive change at PLUS. I will encourage the organization to take smart risk and consider different approaches. I will always listen to members and their concerns. I will always be honest. And, I am sure that I won’t always make everyone happy all the time, but every decision or recommendation I make will be intended to improve members’ lives and help your association.

PLUS: What do you do for fun when you aren’t working?

Robbie: One of the hardest interview questions I have ever faced is what your hobbies are. The answer is I generally have fun working so I do that a lot, and I am having a blast learning about PLUS and the professional liability industry, but I just really don’t have a lot of hobbies or outside interests. And, at this point in time in my life any time not occupied by work is dedicated to my beautiful wife and three amazing kids. I spend most of my free time cheering them on in sports, going to band concerts, playing baseball or soccer in the back yard, or trying to help them with homework. Outside of that you may find me reading a book or watching videos at a coffee shop or sitting in the stands at a Minnesota sports team game. And just so you know this is the Vikings’ year, even though I’ve been wrong about that for almost half a century now.

PLUS Conference 2015

November 11–13
Hilton Anatole
Dallas, TX

The PLUS Conference is the place to connect, learn and find solutions. This year’s program features leading-edge panel discussions with thought leaders and industry experts debating and discussing the emerging risks in the professional liability industry. And once again, the PLUS Conference will feature high-profile keynote speakers to entertain and enlighten attendees. Scheduled to speak:

George W. Bush served as the 43rd President of the United States from 2001 to 2009. After the Presidency, George and Laura Bush founded the George W. Bush Presidential Center in Dallas, Texas. President Bush is also the author of a bestselling memoir, Decision Points, and recently authored a book about his father, President George H.W. Bush, titled 41: A Portrait of My Father.

Daymond John is the CEO and Founder of FUBU, a much-celebrated global lifestyle brand. In 2009 he joined the cast of ABC’s entrepreneurial business show, Shark Tank, by acclaimed producer Mark Burnett.

Diana Nyad is a world-record-holding long-distance swimmer, author, and public speaker. At the age of 64, Diana successfully fulfilled her lifelong dream of completing the 110-mile swim from Cuba to Florida.

Don’t miss it! Register now at www.plusweb.org.
With the recent emergence of several high profile data breaches, one thing has become apparent—frequent, large, costly and destructive privacy breaches have become the new normal. The escalated frequency of these events, which compromise our personal, financial and health information, is a call to action for every organization to decide how they will respond to a data breach. If the headline-grabbing healthcare and retail breaches have not gained enough attention, then the recent June 2015 breach of the U.S. Office of Personnel Management (“OPM”), that impacted nearly 21.5 million people, certainly should. We all must acknowledge: for every organization, it’s not a matter of if, but when.

This article will examine the relief being offered by the federal government to the individuals whose data was compromised in the OPM data breach, whether such relief would be available under proposed federal legislation, and how new federal laws could affect the market for cyber liability insurance.

In June, the U.S. government, via the OPM breach, subjected tens of millions of its citizens to the possibility of identity theft. And that impacted group doesn’t even include the 4.2 million citizens whose social security numbers were stolen from the OPM earlier in April 2015. As we have learned from various government releases, the records that were compromised in the OPM breach not only included social security numbers, but also detailed, sensitive background information, such as employment records, relatives names, personal addresses, and psychological information like past drug abuse or emotional disorders. Over 1.1 million of June’s compromised files included fingerprints, too. The motive of the attack is not certain, but there are a number of nefarious uses for this type of information.

So what is the federal government doing in response to the largest bureaucratic breach in history? So far, it has sent individual notifications to those whose information has been compromised and has offered free full service identity restoration, identity theft insurance and continuous credit monitoring. How did the federal government determine this would be the appropriate response? Simply put: it is hard to tell.

In 2007, the White House issued M-07-16, which requires federal agencies, including OPM, to have in place security protocols for protecting private data and for responding to a breach of that data. M-07-16 mandates that all federal agencies: (1) review their existing requirements with respect to privacy and security; (2) include existing and new requirements for incident reporting and handling; (3) address external breach notification; and (4) develop policies concerning the responsibilities of individuals authorized to access personally identifiable information.

The White House considered six elements as key for any policy and plan that addresses external notification:• whether breach notification is required;• timeliness of the notification;• source of the notification;• contents of the notification;• means of providing the notification; and• who receives notification: public outreach in response to a breach.

In implementing the policy and plan, the Agency Head makes the final decision regarding breach notification, including whether it is even necessary. What the White House did not mandate in M-07-16 is what, if anything, a breached agency should offer those impacted by the breach. In short, there is no mention of credit monitoring or identity theft prevention services. From publicly available information, it is unclear what OPM’s breach response and external notification policy and plan is. So, we have to look elsewhere for possible guidance.

Currently, there is no federal law regulating data breach response. Perhaps OPM looked to several pieces of pending federal legislation in determining how it responded to the breach:

- Data Security and Breach Notification Act of 2015;
- Personal Data Notification and Protection Act of 2015;
- The Personal Data Protection and Breach Accountability Act of 2011;
- Secure and Fortify Electronic Data Act

OPM’s breach response procedures appear to track most closely with the Data Security and Breach Notification Act of 2015 (“the DSBNA”), and/or the Personal Data Notification and Protection Act of 2015, two pieces of proposed legislation that are substantially similar. Under the DSBNA, companies will not be required to provide notice if there is no reasonable risk of identity theft, economic loss, or economic or financial harm. If notification is deemed necessary, companies would be required to provide that notice to affected individuals within 30 days after discovery of a breach.

The DSBNA also would remove the possibility of individual civil suits, permitting only the attorney general to file a suit regarding a data breach. However, what the proposed legislation does not require is for a breached company to provide free ID theft protection services, such as credit monitoring, identity monitoring or fraud alerts. Significantly, the DSBNA also provides for complete preemption of state laws.

The irony here is that, through preemption, the DSBNA would deny individuals affected by a breach statutory access to free credit monitoring or other identity theft protection services, when that is exactly what the federal government determined was the best response to the OPM breach. Maybe OPM was trying to take a measured approach, taking into consideration both the pending federal legislation and also their ongoing review of how the states have been handling breaches. And maybe, by offering credit or identity...
monitoring, something the pending federal legislation does away with, the federal government is signalling that it actually values the measures most states have implemented and values how the states have handled breaches so far. Is credit or identity monitoring the best and only reasonable response for a breach of this kind? Could OPM’s offer of credit monitoring be signalling something even bigger: that the proposed legislation may be modified so that it does not preempt the states’ rights?

The issue of preemption is extraordinarily important to a number of states and can sometimes create quite the constitutional hazard. With the exception of Alabama, New Mexico and South Dakota, every other state, as well as the District of Columbia, Puerto Rico and the U.S. Virgin Islands, have enacted legislation requiring notification of security breaches involving personal information.

On July 7, 2015, the National Association of Attorneys General wrote to congressional leaders pleading for the DSBNA not to preempt their authority within their respective states.10 The AGs detailed how they themselves are best equipped to help their citizens, proclaiming that, “States are the front line in helping consumers deal with the repercussions of a data breach.” According to the letter, the AGs are able to regularly check if data collectors are equipped to handle breaches themselves. The federal government has not yet responded to the AG’s pleas.

Preemption also is not the only way to travel down the path of consistent federal breach response laws. We’ve been down this road before. The privacy requirements of the federal Gramm-Leach-Bliley Act of 1999, which addresses consumer financial issues, and the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) already set the scene with respect to privacy in terms of what’s required by companies but do not preempt state law. With HIPAA as an example, if a HIPAA standard, requirement, or implementation specification is contrary to a provision of state law, the HIPAA Provision generally preempts the provision of state law unless state law relating to the privacy of individually identifiable health information is more stringent than the HIPAA Provision.11 A state law is more stringent than a HIPAA provision if the law prohibits or restricts a use or disclosure that would otherwise be permitted under HIPAA.12 Thus, if a state law authorizes only certain limited uses and disclosures and excludes those permitted under HIPAA, then the state law is more stringent than HIPAA and is not preempted.13 Accordingly, an entity subject to both a more stringent state law as well as HIPAA would be obligated to comply with the more stringent state law.14 Specific examples in the breach response context would be accelerated notification deadlines, state specific content requirements in the notification letter and state attorney general/consumer agency notification. These items are not required under HIPAA but are viewed as more restrictive and providing more protection for the affected individuals.

What does all of this mean for cyber liability insurance? Currently, cyber liability insurance is priced to provide for many of the costs of complying with the various state laws following a breach, and as more states have enacted breach response laws, the overall cost of breach response has risen. Moreover, most insurers have built their expertise and have set up their cyber liability services based on the state-by-state approach. Would standardized breach response laws help streamline coverage in breach response policies and lower the cost of the insurance? Risk management groups, including RIMS, seem to think so. In fact, RIMS has lent its support to both the DSBNA and the Personal Data Notification & Protection Act of 2015. The DSBNA would possibly lead to less confusion for consumers and perhaps lower cyber liability premiums, but only if the federal government is truly prepared to completely preempt the 47 states that already have considered laws on the books. If there is no preemption, then the state of affairs will only become more complicated and potentially more costly. The DSBNA, and federal legislation like it, are certainly something to keep our eye on.

Endnotes

1 Special thanks go to Alan Fiano, Leah Saltzman and Maxwell Frenkel for their kind assistance in the preparation of this article.

2 Full service identity theft restoration and identity theft insurance was offered to those who had personnel information impacted. The same, plus continuous credit monitoring and fraud monitoring service, beyond credit files, was offered to those who were impacted by the background investigation incident. See https://www.opm.gov/cybersecurity.


4 M-07-16 provides two threshold questions for an agency to determine if notification should be provided: what is the likely risk of harm and what is the level of impact. It provides little guidance beyond this, leaving the ultimate decision to notify up to the federal agency.

5 On March 25, 2015, the United States House of Representative, Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade approved a draft of this legislation which would replace state data breach notification laws with a national standard.

6 Proposed by President Obama in January 2015, provides that notification shall be made without unreasonable delay, not exceeding 30 days, unless necessary for law enforcement or with an extension granted by the FTC of up to 30 days. Provides that a business entity is exempted from notice requirements if a risk assessment concludes that there is no reasonable risk of harm to the affected individuals. If notification is required to more than 5,000 individuals, the business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis within 30 days. It also gives the FTC rulemaking authority and the AGs the right to bring enforcement actions.

7 Introduced by Sen. Richard Blumenthal, D-Conn., this legislation is intended to protect consumers from threats to their sensitive, personally identifiable information online and to safeguard data security. It has been referred to the Senate Judiciary Committee.

8 Introduced in July 2015, the House Energy and Commerce Committee’s trade subcommittee approved the bill but it has been in Committee ever since.

9 When state law and federal law conflict, federal law displaces, or preempts, state law, due to the Supremacy Clause of the Constitution. U.S. Const. art. VI., § 2. Preemption applies regardless of whether the conflicting laws come from legislatures, courts, administrative agencies, or constitutions.


11 45 C.F.R. §§ 160.201; 160.203.

12 Id.

13 Id. See also Nat’l Abortion Fed. v. Ashcroft, No. 04 C 55, 2004 WL 292079 (N.D. Ill. Feb. 4, 2004) (noting that an Illinois medical privacy law containing a list of permissible uses and disclosures that excludes uses and disclosures permissible under HIPAA is not preempted because it is more stringent than HIPAA).

14 Id.
Retaliation under the National Labor Relations Act: The Next New Wave of Claims, for Both Union & Non-Union Employers?

By Kim P. Bush, Esq. & Ellen R. Storch, Esq.

Until recently, non-union employers had little reason to consider the National Labor Relations Act (the “Act”), as they rarely faced liability under its provisions. They typically only took notice of the Act or the federal agency charged with enforcing it, the National Labor Relations Board (the “NLRB”), if their workers threatened unionization.

However, the NLRB has forced non-union employers to turn their attention to the Act with a slew of recent decisions holding that employer policies violate workers’ rights to engage in “concerted and protected activities”. This should interest the underwriting and broker communities as Employment Professional Liability Insurance (“EPLI”) coverage can be triggered if workers allege that employers retaliated against them for violating such policies.

The Act preserves the right of all private-sector employees, whether union or non-union, to engage in protected concerted activity.1 Section 8(a)(1) makes it an unfair labor practice for an employer “to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7” of the Act. In turn, Section 7 guarantees employees the right to engage in “concerted activities for the purpose of collective bargaining or other mutual aid or protection.” “Concerted activities” occur when two or more employees act together to improve any term or condition of employment. According to the NLRB, concerted activity can occur in surprising ways, such as when a worker “likes” a co-worker’s status or comment on Facebook, or retweets a co-worker’s comments on Twitter.

This article describes the evolving role of the NLRB, the scope of employer (and carrier) liability for retaliation claims, how claims arise and proceed, the NLRB’s views on specific employer policies, and how employers and carriers can minimize risk of liability.

The NLRB’s Evolving Role and Focus

Created in 1935, the enforcement activities of the NLRB were historically associated with labor unions and collective bargaining. However, over time, traditional unionization activities have steadily declined.2 As a result, the visibility, power, influence and necessity of the NLRB and the Act decreased. In recent years, the NLRB has reinvented itself and has undergone a generational renaissance to capture a new economy of young, technologically savvy workers.

To appeal to a new generation of superconnected and mostly non-union workers, the NLRB released a mobile app, advertised as an “interactive wizard.” The app teaches workers about their rights under the Act, and can connect them right to the NLRB to file a charge.

The NLRB has also zeroed in on employer attempts to limit the social media activities of its workers. In 2011, the NLRB Actig General Counsel issued a report detailing 14 cases involving the social media policies of employers. In this report, the NLRB weighed in on “the protected and/or concerted nature of employees’ Facebook and Twitter postings . . . and the lawfulness of employers’ social media policies and rules.”3 The decisions held employer policies to be unlawful if they could be construed as prohibiting concerted activities on social media.

The NLRB then expanded its focus, and what followed was an avalanche of colorful and murky decisions opining on the lawfulness of all types of employer policies. This year, the NLRB’s Office of the General Counsel released a report purporting to clarify its position on the lawfulness of policies (the “Memorandum”).4 Unfortunately, the Memorandum may have created more confusion than clarity, as it is difficult to understand the reasoning as to why certain seemingly benign policies are deemed unlawful and others lawful.

For employers, the NLRB’s recent decisions holding that certain employee handbook provisions violate the Act have created a virtual minefield, the pitfalls of which remain increasingly difficult to map and avoid. The question for insurance carriers becomes whether the NLRB’s decisions foreshadow the need to reassess potential risk and exposure under current EPLI policies.

What is the Scope of Employer Liability & by Implication Carrier Liability?

Remedies available to an employee who establishes retaliation under the Act can include reinstatement, back pay and interest. In extreme cases, the NLRB has also awarded front pay and attorneys’ fees.5 The NLRB can also require the employer to rescind the policy and post a notice to employees. The notice advises employees of the role of the NLRB, and provides information about filing charges, potentially prompting the filing of additional charges and creating more liability.

Although most EPLI policies have exclusions that preclude coverage for claims for violations of the Act, many such exclusions provide a carve-back specifying that the exclusion does not apply to claims alleging retaliation under the Act. This carve-back could trigger coverage for a claim by an employee that he was terminated, harassed, discriminated against, or suffered other adverse action in retaliation for engaging in concerted activity. This type of claim might preserve coverage under an EPLI policy for an action pending before the NLRB which, in addition to covering an award of back-pay (and possibly front pay and attorneys’ fees), would also cover defense costs associated with litigating before the NLRB, which can become very costly very quickly.

How do Claims Arise and Proceed?

Retaliation claims under the Act implicating handbook provisions may arise when an employer terminates an employee for violating a policy. The employee may file an unfair labor practices charge with his regional NLRB office, claiming that he was terminated in retaliation for engaging in protected

continued on page 14
Supreme Court finally made clear the standards for analysis for both halves of the “false or misleading statement” element.

**Omnicare’s Second Prong Is Simply the Misleading Half of “False or Misleading Statement” Element**

Indeed, the “misleading” half of the “false or misleading statement” element was the real showdown in *Omnicare*. At oral argument, it seemed inevitable that the Supreme Court would reject the plaintiffs’ argument that a genuinely believed opinion may nonetheless be considered “false” if it is later determined that the opinion was incorrect. But the Court also expressed discomfort with the potential loopholes created by Omnicare's position at the other extreme—that if a statement is phrased as an opinion, it cannot be found to be either false or misleading under the securities laws, as long as the opinion was honestly held by the speaker.

There were many wrong turns that the Court could have taken in rejecting these two extremes, running the risk of further confusing the law not only regarding the truth or falsity of opinions, but also muddling the law of scienter and materiality. Several of these potential wrong turns were raised at oral argument and in the briefing to the Court—such as the Solicitor General's suggestion that argument and in the briefing to the Court—potential wrong turns were raised at oral argument. Thus, the law on what can make a statement of opinion misleading inevitably would have developed in the courts, with or without *Omnicare*. For this simple reason, the view that *Omnicare’s* second prong is something new and plaintiff-friendly is wrong; it is simply the pre-existing “misleading” half of the “false or misleading statement” element.

And *Omnicare* did not only correctly restate the standard for showing a statement is “misleading,” it elaborated on that standard in a way that will greatly help defendants argue for dismissal of claims based on statements of both fact and opinion. In evaluating what a “reasonable investor” would understand, the Court directed courts to consider the entire factual context in which defendants made the challenged statement. In particular, the Court emphasized that whether a statement is misleading “always depends on context,” so a statement must be understood in its “broader frame,” including “in light of all its surrounding text, including hedges, disclaimers, and apparently conflicting information,” and the “customs and practices of the relevant industry.”

A good motion to dismiss has always analyzed a challenged statement (of fact or opinion) in its broader factual context to explain why it was not misleading. But many defense lawyers unfortunately leave out the broader context, and courts sometimes take a narrower view. Now, this type of superior, full-context analysis is explicitly required by *Omnicare*. Combined with *Tellabs*’ directive that courts consider scienter inferences based not only on the complaint’s allegations, but also on documents on which the complaint relies or that are subject to judicial notice, courts clearly must now consider the full array of probative facts in deciding both whether a statement was false or misleading and, if so, was made with scienter. Plaintiffs cannot cherry-pick what the court considers anymore.

In the full context of the facts, *Omnicare* prescribes strict scrutiny of misleading-statement allegations, emphasizing the narrowness of its standard: an opinion is not misleading just because “external facts show the opinion to be incorrect,” if a company fails to disclose “some fact cutting the other way,” or if the company does not disclose that some disagree with its opinion. Rather, the Court seized upon the misleading-statement analysis that the *amicus* brief we filed on behalf of the Washington Legal Foundation (alone among the parties and amici) had urged, finding that an opinion is misleading only if it omits information necessary to avoid creating a false impression of the “real facts” in a reasonable investor, when the statement is taken as a whole and considered in its full context. Unlike the “reasonable basis test” urged by the Solicitor General, the Court emphasized that this inquiry “is objective.” And the Court stressed that pleading a misleading opinion will be “no small task for an investor.”

**Conclusion**

Far from being plaintiff-friendly, *Omnicare* has expressly given the defense bar tools with which to make better arguments, in a wide-range of cases beyond those involving Section 11, or beyond even statements of opinion. If the defense bar uses *Omnicare* correctly, the decision will have a profound impact on securities litigation defense and, more importantly, on the ability of directors and officers to speak their minds without fear of liability for doing so honestly.

---

**Endnotes**


4 501 U.S. at 1095.

5 886 F.2d 1109 (9th Cir. 1989).

6 551 F.3d 1156 (9th Cir. 2009).

7 655 F.3d 105 (2d Cir. 2011).

8 See, e.g., *Brody v. Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002) (a statement is misleading due to omissions if it “affirmatively create[s] an impression of a state of affairs that differs in a material way from the one that actually exists”).

9 135 S. Ct. at 1320.

10 135 S. Ct. at 1328.

11 *Id.* at 1329-30.

12 *Id.* at 1327.

13 *Id.* at 1332.
render the limitations period meaningless and could even expose current fiduciaries to liability for decisions made decades ago. The Ninth Circuit also found that the district court had properly allowed plaintiffs the opportunity at trial to prove that “changed circumstances” occurring within the limitations period would have prompted a full “due diligence” review and, in turn, led prudent fiduciaries to replace the existing mutual funds. Because the plaintiffs had failed to prove such changed circumstances, however, the Ninth Circuit affirmed the district court’s ruling that the plaintiffs’ claims were time-barred. The Tibble plaintiffs thereafter filed a petition for certiorari, which the Supreme Court accepted.

The Supreme Court’s Opinion

The Supreme Court framed the question as “whether a fiduciary’s allegedly imprudent retention of an investment is an ‘action’ or ‘omission’ that triggers the running of [ERISA’s] 6-year limitations period.” In answering this question, the Court found that the Ninth Circuit had erred in failing to consider that under trust law, “a fiduciary is required to conduct a regular review of its investment with the nature and timing of the review contingent on the circumstances.” The Court observed that “a trustee has a continuing duty to monitor trust investments and remove imprudent ones,” and that this duty exists “separate and apart from the trustee’s duty to exercise prudence in selecting investments at the outset.”

Thus, the Court held that a plaintiff may allege a separate breach of fiduciary duty claim under ERISA for the failure “to properly monitor investments and remove imprudent ones” and that such a claim would be timely so long as the alleged breach of this duty occurred within six years before filing suit. The Court expressly declined to opine on the scope of the duty to monitor, noting that the parties “disagree[d]” as to “the scope” of that duty. The Court remanded the case to the Ninth Circuit to consider whether the plan fiduciaries had “breached their duties within the relevant 6-year period under § 1113, recognizing the importance of analogous trust law.”

Implications for Fiduciaries and Their Insurers

Certain aspects of Tibble are unremarkable from a fiduciary perspective. Most fiduciaries would have agreed pre-Tibble that they have a duty to periodically monitor a plan’s investment options. The scope of what that duty entails remains an open issue, though the Supreme Court did observe rather broadly that a trustee “must systematically consider all the investments of the trust at regular intervals to ensure they are appropriate,” and that if a trust includes assets that are inappropriate investments, “the trustee is ordinarily under a duty to dispose of them within a reasonable time.”

From a litigation perspective, Tibble will undoubtedly make it more difficult to dispose of imprudent investment claims on timeliness grounds in cases where the plan selection decision was outside the limitations period. Plaintiffs will frame these claims in terms of a breach of the duty to monitor plan investments rather than as traditional imprudence claims. Further, while Tibble was limited to claims involving investments, the plaintiffs’ bar will likely view the Court’s decision as opening the door to a broader universe of “failure to monitor” claims against fiduciaries. As such, fiduciaries, plan sponsors and their insurers can expect an increase in litigation costs in these cases. The ultimate viability and value of these failure-to-monitor claims, however, is still uncertain at this point. The Ninth Circuit’s decision on remand should provide further guidance on the exact contours of such a claim and whether the “changed circumstances” or red flag analysis becomes part of the threshold elements of such a claim.

While the courts grapple with Tibble, now may be a good time for plan sponsors and fiduciaries to revisit their existing processes and procedures for monitoring the continued prudence of ERISA plan investments and other plan-related decisions. While courts have agreed that fiduciaries are not obligated to “scour the market” for the cheapest possible investments (and presumably the same holds true for other plan-related decisions), a well-documented decision-making and review process for all plan decisions, including decisions not to implement a particular course of action, can go a long way in demonstrating that plan fiduciaries have fulfilled their ERISA obligations. In this respect, Tibble is a good illustration. The fiduciaries prevailed on the vast majority of plaintiffs’ claims based on a solid record demonstrating a prudent process with respect to the plan’s investments. On the other hand, with respect to the three retail class mutual funds for which the court found liability, the district court and Ninth Circuit both found the record lacking with respect to the fiduciaries’ process.

Endnotes

4 See, e.g., Fuller v. SunTrust Banks, Inc., 744 F.3d 685, 697-702 (11th Cir. 2014); Tibble v. Edison, Int’l, 729 F.3d 1110, 1119 (9th Cir. 2013); David v. Alpin, 704 F.3d 327, 340-43 (4th Cir. 2013).
5 See Fuller, 744 F.3d at 702; Tibble, 729 F.3d at 1120; David, 704 F.3d at 340-43.
6 The plaintiffs also challenged the practice of revenue sharing associated with the plan’s funds and claimed that offering a unitized stock fund, money market-style investments and mutual funds, had been imprudent.
9 729 F.3d at 1130-37. 10 Id. at 1120. 11 Id.
12 135 S. Ct. at 1826. 13 Id. at 1828. 14 Id.
15 Id. at 1829. 16 Id. (citations omitted).
17 See Hecker v. Deere & Co., 556 F.3d 575, 586 (7th Cir.), pet. for reh’g and reh’g en banc denied, 569 F.3d 708 (7th Cir. 2009), cert. denied, 130 S. Ct. 1141 (2010); Tibble, 729 F.3d at 1135; cf. Braden v. Wal-Mart Stores, Inc., 588 F.3d 585, 596 (8th Cir. 2009) (acknowledging that a fiduciary might “have chosen funds with higher fees for any number of reasons, including potential for higher return, lower financial risk, more services offered, or greater management flexibility”).
18 For example, the fact that fiduciaries secured independent advice from a consultant was some evidence of a thorough investigation, but did not offer any evidence regarding the specific recommendations made by the consultant or the basis for the consultant’s advice. The court also rejected the fiduciaries’ argument that mandatory investment minimums precluded them from selecting institutional share classes for these funds, finding that the fiduciaries should at least have inquired whether the fund managers would waive those minimums in light of substantial evidence (including testimony from the fiduciaries’ expert witness at trial) that such waiver requests would have been granted. See Tibble, 729 F.3d at 1137-39.
PLUS essentials is the newest educational offering from PLUS—an online platform that presents PLUS’ industry-leading educational content in an interactive and engaging format. PLUS essentials is an outgrowth of PLUS University, an on-site program that utilizes material from the PLUS curriculum and has been offered since 2007. While PLUS University has been a very popular program, companies are not always able to take advantage of it for all new hires. That is where PLUS essentials comes in.

These courses, each of which take between 60 to 90 minutes to complete, are designed for individuals new to our industry, and provide a solid foundation of knowledge regarding professional liability insurance and key coverage lines. The online presentation makes learning with PLUS essentials fun—the interactive text with integrated audio and video keeps students’ attention while the real-time quizzes provide instant feedback and proof of learning.

**The five PLUS essentials modules are:**

**History of Professional Liability Insurance (PLI).** This course provides students with a clearer understanding of the insurance products with which they work, and the tools to help them identify and better address their clients’ coverage needs. It introduces learners to the need for PLI, the history of the PLI industry, and how the industry is structured. From these basic building blocks, learners are introduced to the types of professionals who work in the industry, and the significant tort reforms that have changed the industry over time.

**Commercial General Liability (CGL) Insurance Basics** explains why businesses need this type of coverage and explains the historical development of liability coverage. Students learn which types of exposures CGL insurance responds to, the coverages that are provided in a CGL policy, and why it does not respond to professional liability exposures. Finally, it introduces Excess and Umbrella Liability Insurance and explains the similarities and differences between these types of coverage.

**PLI Concepts** provides a glimpse into some features that are unique to Professional Liability Insurance (PLI). Learners become familiar with conditions that alter coverage, important exclusions, policy limitations, and who controls the defense when there is first dollar or a high deductible or SIR applies. Students see how the PLI policies work, who is covered under a PLI policy, and how they can be tailored for a variety of professional services. Learners also review important considerations for underwriters, and ways the insurer and insured can mitigate risk. Anyone starting out in professional liability or moving into a career in PLI from other lines of insurance will benefit from taking this course.

**Introduction to Directors and Officers Liability Insurance** provides an overview of Directors and Officers Liability Insurance (D&O), including key reasons why D&O insurance is essential for directors and officers today. Learners become familiar with the responsibilities and duties that directors and officers owe to their organizations, as well as other factors that should encourage organizations to carry D&O liability insurance. The course also covers how D&O policies work, including the concept of indemnification and how it relates to advancement and defense costs. Learners study the various sources of liability, including state and federal laws, Sarbanes-Oxley (SOX), and reforms such as the Private Securities Litigation Reform Act (PSLRA).

**Introduction to Medical Professional Liability Insurance** provides a brief history of MedPLI and an overview of the facilities and individuals that MedPLI protects. The course reviews the two main forms of coverage—occurrence and claims-made—and why claims-made coverage is preferable for long tail exposures. Students learn which policy provisions are key to analyzing the coverage provided on these policies, and the similarities and differences between Hospital Professional Liability (HPL) and Physicians Professional Liability (PPL), including exposures they cover, how coverage is rated, and common types of Med-PL claims. It also touches on exposures that dentists and other allied healthcare professionals face.

Students receive documentation of successful completion of each course, and can take an exam at a testing center to obtain Continuing Education (CE) credits. The exam covering the five-part program is available and approval of CE filings is in process.

case law frustrates the student of the subject. Jurisdiction is problematic across state lines. Though most commentators take the position that the care is provided at the patient’s location, and that the courts of his state therefore have jurisdiction, this theory has not been much tested either. With respect to venue, one locale may have plaintiff-oriented judges and juries; another may not. Although most states have adopted a national standard of care, some retain state standards, and a few define the standard as the custom within the defendant’s locality or like localities. If a doctor from a state with a national standard provides distance care to a patient in a state embracing the locality standard, which standard applies—and from what pool can experts be selected? Then too, even where the standard’s definition is clear, technological evolution will mean that its practical application will change over time. State statutes, rules and regulations governing telemedicine also vary by jurisdiction. Plaintiffs will argue, of course, that the standard of care using telemedicine technology is the same as it is when a physical exam is conducted in person. Some states have, in fact, codified the standard of care accordingly. As of this writing, however, in no state has the court of last resort tested this notion under common law.

Many specialty societies have promulgated guidelines or other documents on the use of telemedicine. The American Telemedicine Association has done so as well. More are under development. While in theory these statements can help minimize risk if used appropriately, plaintiffs can argue that they establish the standard of care. There is evidence, in fact, that such guidelines are used more often as a sword than as a shield. The problem is aggravated by the fact that as of four years ago there were already more than 2700 clinical practice guidelines promulgated by more than 350 groups, and among them there were many inconsistencies. No doubt there are many more now. The problems with guidelines do not end there: they tend to be inflexible, they are vulnerable to rapid obsolescence, they are often vague, they frequently fail to specify the basis for any given recommendation, and they are often written by authors with conflicts of interest, such as ties to industry. There is not even a consensus on the meaning of “evidence-based.”

Claims Scenarios

As noted, telemedicine-related claims have been very few in number. One must resort to polling carriers and defense counsel to find the few that have been filed. Because teleradiology has been one of the most prevalent modes, claims to date can often fall under that category. Allegations include:

- Incorrect interpretations of diagnostic images of various types by a radiologist, from home or some other remote location;
- Miscommunication over the timeliness of the required reading: e.g. a “stat” reading was requested but not provided;
- Failure to communicate presenting symptoms to a remote, examining neuro-radiologist; failure to timely diagnose a spinal abscess resulting in permanent impairment;
- Incorrect remote reading of fetal monitoring strips by an obstetrician;
- Suspected stroke incorrectly diagnosed by a tele-stroke consult;
- Failure to adequately remotely monitor and assess an ICU patient for blood loss and hypotension resulting in severe brain damage; failure to summon an intensivist for a more thorough bedside evaluation.

Other Potential Telemedicine Allegations:

- Exam should have been performed in-person rather than by videoconference.
- Image distortion causing misdiagnosis
- Incomplete telemedicine examination
- Power failure during a consult causing delay/error
- Negligent prescribing based on a video examination
- Negligent failure to provide telemedical support

Licensure and Scope of Practice

Historically, states regulate health care professionals through licensure. The professional’s license is an indication of some basic level of qualification, and the main tool states use to promote satisfactory physician performance. Without a valid license, a health care professional may not lawfully serve patients except in emergencies and other special circumstances. Even in emergencies, some states permit practice without a license only if services are provided pro bono. Generally, licenses are valid only within the state of issuance.

A telephysician must be mindful of this restriction. If he serves a patient in a state where he holds no license, he may be accused of unauthorized practice. As the law stands now, doctors wishing to see patients in a variety of states should be licensed in all of them. A number of legislative proposals have been crafted to obviate the need for multiple licenses, but none has been enacted as yet. The Federation of State Medical Boards (“FSMB”) has created an Interstate Medical Licensure Compact that still contemplates licensure in each state where a physician practices, but that makes the associated administrative burden somewhat easier. As of this writing, some eleven states have enacted the Compact into law. The expense and inconvenience of maintaining a series of licenses, each subject to different rules, are burdens outweighed by the risk of practicing without a license.

Health care providers (“HCPs”) must also conform to scope of practice requirements, which may also vary state-to-state. For example, in Virginia, a nurse practitioner may interact with her collaborating physician by electronic communications, but that may not be true in other states. Virginia physicians’ assistants enjoy no such freedom. The professional needs to become acquainted with the varying requirements in each state where she practices.

Credentialing and Privileging

A hospital’s Board of Directors is ultimately responsible for its credentialing and privileging decisions. Credentialing refers to obtaining, reviewing, and confirming a HCP’s credentials and professional documentation; privileging refers to an organization’s judgment, based on peers’ evaluations of a HCP’s credentials and performance, on the scope and content of patient care services that the HCP may provide within its walls. In conventional care, a physician submits his credentials and the Board’s delegate, usually a committee of the medical staff, decides whether to grant privileges or not and, if granted, their extent. If the credentialed physician wishes to serve patients at another hospital, however, his existing privileges generally are insufficient to permit that, and he has to go through the same process again. Much of telemedicine’s value lies in bringing expertise from large centers to smaller ones. Until fairly recently, however, even a highly qualified doctor at a major medical center willing to assist inpatients elsewhere would be obliged to go through the credentialing process at the smaller hospital. Under Federal “Conditions of Participation” regulations promulgated in 2011, however, so long as specified requirements are met, the smaller hospital may, in large part, rely upon the credentialing decisions made at the larger.
Privacy and Confidentiality

Few data are more sensitive and private than medical records, especially those that document psychiatric care, sexually transmitted diseases, and other delicate topics. Hackers can and do invade data at the Pentagon; recent headlines have repeatedly reported data breaches, sometimes massive, at health care institutions and insurers. Both federal (HIPAA\(^\text{18}\), HITECH\(^\text{19}\), COPPA\(^\text{20}\)) and state law prohibit such conduct; moreover, ethical principles condemn them as well. Intentional misconduct aside, simple human error, the commonest mechanism of privacy breaches, is both unlawful under state and federal statutes and actionable at common law. No exception exists for distance care. Of course, traditional paper records are far from risk-free as well, but those wishing to serve patients at a distance should be at pains to identify and ameliorate risk. The consequences for failing to do so may be severe.

Fraud and Abuse

The Stark law\(^\text{21}\) and the anti-kickback statute\(^\text{22}\) apply to telemedicine just as they do to in-person care. Several OIG opinions deal explicitly with telemedical arrangements,\(^\text{23}\) and those should be consulted if, for example, a hospital wishes to provide a physician with some of the equipment needed to perform distance care services.

FDA

To some extent, telemedicine relies upon devices used for diagnosis and sometimes treatment. A large and ever-growing number of mobile apps is on the market, most of which have not been validated in clinical trials nor approved by FDA. So far, FDA has taken a fairly restrained approach, and stayed its regulatory hand to, it seems, encourage the growth of the technology. Apps that are not devices at all, such as a medical textbook made available electronically, are not regulated. Others that could be are not, at least at present; FDA seems to be focused only on apps that could influence diagnostic or management decisions as opposed to, for example, apps intended to prevent disorders from arising or to encourage fitness.\(^\text{24}\)

Conclusion

Telemedicine has a bright future, and will facilitate access to care as few other technologies can. It is increasingly popular for its convenience and low cost. Its growing popularity, however, will undoubtedly give rise to tort claims. Moreover, it is subject to extensive regulation. For risk management and claims defense purposes, insurers willing to underwrite these risks and providers seeking to offer distance care should acquaint themselves with relevant law.

Endnotes


10. See, e.g., Hyams et al., 122 Ann. Int. Med. 450, 451-52 (1995)(Only 17 of 259 claims reviewed (6.6%) involved clinical practice guidelines; of these, in 12 the guidelines were inculpatory and in 4, exculpatory); Mehliman, 40 J.L. Med. & Ethics 286 (2012) (In 24 additional reported cases, the defense used guidelines successfully in 9 and the plaintiffs in 11).

11. Institute of Medicine, Clinical Practice Guidelines We Can Trust 146 (2011).


15. Id.

16. “Collaboration and consultation among nurse practitioners and patient care team physicians may be provided through telemedicine as described in § 38.2-3418.16.” Va. Code Ann. § 54.1-2957.


23. See, e.g, OIG Advisory Opinions Nos. 11-12, 99-14, and Op. 02-12.

National Labor Relations Act continued from page 8

and concerted activity—and that the employer policy was unlawful. The charge is investigated by regional office attorneys. If they believe that the Act has been violated, they also prosecute the claim, before an NLRB administrative law judge. Thus, the NLRB effectively acts as investigator, prosecutor and adjudicator.

Recent NLRB Pronouncements on Various Types of Employer Policies

In order to determine whether a policy violates the Act, the NLRB first considers whether it explicitly restricts activities protected by Section 7. If so, the rule is unlawful. If it does not, the rule is still unlawful if employees could “reasonably construe the language to prohibit Section 7 activity,” or it has actually been used to restrict exercise of that activity. While this guiding legal principle appears to provide a framework for anticipating how the NLRB would interpret employer policies, the NLRB has taken an increasingly broad and unpredictable view of how employees could “reasonably construe” a policy to infringe on their right to engage in concerted activity.

- **Handbook Provisions Prohibiting Harassment and Discrimination**

  Guided by United States Supreme Court precedent, employers regularly distribute policies prohibiting harassment and discrimination. However, according to the NLRB, these policies can violate the Act. For example, the Memorandum deemed unlawful a policy prohibiting “defamatory, libelous, slanderous or discriminatory comments about the company, its customers and/or competitors, its employees or management.” However, the Memorandum considered lawful the following rule: “being insubordinate, threatening, intimidating, disrespectful or assaulting a manager/supervisor, coworker, customer or vendor will result in discipline.” The Memorandum explained that employees might think the first rule bans criticism of their employer; however, the second rule was lawful because employees should understand that it only prohibits serious misconduct, like threats and assault.

  Notably, the Memorandum deemed unlawful standard provisions in anti-harassment policies, including one prohibiting employees from sending “unwanted, offensive or inappropriate” e-mails, and another advising employees that: “Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by e-mail.” The NLRB’s rationale was that these rules were too vague and employees might believe they prohibited the sending of communications that were protected. Confusingly, the Memorandum approved a policy stating that any logos or graphics worn by employees “must not reflect any form of violent, discriminatory, abusive, offensive, demeaning, or otherwise unprofessional message.” The distinction offered by the NLRB was that this policy merely required professionalism of employees, and did not mention management or the company.

- **Policies Protecting Company Confidential Information**

  Though maintaining the confidentiality of a company’s proprietary information is a long recognized and judicially enforced employee obligation, the NLRB has recently deemed certain confidentiality policies unlawful under the Act. For example, in a recent decision regarding the employee policies of Macy’s, the
NLRB found the store’s confidentiality policy overbroad and unlawful to the extent it required employees to maintain as confidential the “personal information” of employees, “including their names and home and office contacts.” The NLRB found that the provision “obviously restricts employees in their Section 7 rights to discuss their terms and conditions of employment with fellow employees, as well as their ability to notify a union of other employees of [Macy's] who might be interested in participating in the union movement.”

As well, in the Memorandum, the NLRB said it was unlawful for an employer to advise employees: “Never publish or disclose the Employer’s or another’s confidential or property information.” Yet, the Memorandum deemed lawful a policy prohibiting “unauthorized disclosure of business secrets or other confidential information.” The fine distinction, according to the Memorandum, was that the policy prohibiting disclosure of “another’s” confidential information could be read to prohibit employees from disclosing the wage information of another worker.

- Policies Prohibiting Disparagement, Disrespect and Defamation

Employers often prohibit employees from disparaging the company or acting disrespectfully towards management, on social media and elsewhere. The NLRB has found certain such policies unlawful, because they could be construed by employees to prohibit protected behavior. According to the NLRB, discussions among workers about supervisors or wages are “protected concerted activity,” even if they are disparaging or disrespectful. Indeed, the NLRB has held that even defamatory statements by employees can be considered protected, unless they are “maliciously” false.

While the NLRB has held that employers may require workers to act courteously and professionally towards customers, and can prohibit outright insubordination to management, it is difficult to flesh out where the NLRB thinks policies cross the line by prohibiting protected activity. For example, the NLRB approved an employer rule requiring employees “to work in a cooperative manner with management/supervision, coworkers, customers and vendors.” Confusingly, a company policy mandating that employees “be respectful to the company, other employees, customers, partners, and competitors” was unlawful according to the NLRB. According to the NLRB, the first rule simply mandates cooperation while the second could be interpreted as banning criticism of the employer.

**Employer and Carrier Take-Aways**

Many employers attempt to avoid liability under the Act by including a “savings clause” in their handbooks, wording such as, “nothing herein is intended to violate any employee rights protected by the National Labor Relations Act.” However, in the recent Macy’s case, the NLRB held that Macy’s savings clause did not render the challenged policies lawful, because it did not specifically reference the policy provisions that were not intended to violate the Act. As well, Macy’s did not distribute the savings clause until seven months after it distributed the policies. Accordingly, employers should include savings clauses in handbooks, but they should specifically cross reference the policies that could be interpreted as violating Section 8, and they should be distributed concurrently with handbooks. In their confidentiality policies, employers should narrowly define what type of information is being protected, such as trade secrets and customer information. Employers should revise any policy that could be interpreted as restricting employees from disclosing information about wages, labor violations or terms and conditions of employment.

In policies that regulate employee behavior, employers can likely require civil and professional behavior towards coworkers and customers, and can prohibit outright insubordination. However, employers should use caution when limiting employees’ rights to be critical of management. Underwriters typically inquire as to whether an applicant for EPLI insurance has an employee handbook. In light of the NLRB’s aggressive activities, however, underwriters might consider going a step further, and find out if the handbook has been recently reviewed and updated by employment counsel, and whether the applicant has trained its executives, management, and supervisors on the new legal issues under the Act.
Calendar of Events

Chapter Events*

<table>
<thead>
<tr>
<th>Chapter Event</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada Chapter</td>
<td>September 16, 2015</td>
<td>Networking Reception • Montreal, QC</td>
</tr>
<tr>
<td>Eastern Chapter</td>
<td>September 21, 2015</td>
<td>Educational Seminar • New York, NY</td>
</tr>
<tr>
<td></td>
<td>December 9, 2015</td>
<td>Winter Social • New York, NY</td>
</tr>
<tr>
<td>Hartford Chapter</td>
<td>December 2015</td>
<td>Networking Reception • Hartford, CT</td>
</tr>
<tr>
<td>Mid-Atlantic Chapter</td>
<td>September 24, 2015</td>
<td>3-on-3 Basketball &amp; Networking Reception • Philadelphia, PA</td>
</tr>
<tr>
<td></td>
<td>December 2015</td>
<td>Educational Seminar and Holiday Party • Philadelphia, PA</td>
</tr>
<tr>
<td>Midwest Chapter</td>
<td>December 8, 2015</td>
<td>Holiday Party • Chicago, IL</td>
</tr>
<tr>
<td>New England Chapter</td>
<td>September 17, 2015</td>
<td>Educational Seminar • Boston, MA</td>
</tr>
<tr>
<td></td>
<td>December 2015</td>
<td>Holiday Party • Boston, MA</td>
</tr>
<tr>
<td>North Central Chapter</td>
<td>Fall 2015</td>
<td>Educational Seminar • Minneapolis, MN</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>TBD • Minneapolis, MN</td>
</tr>
<tr>
<td>Northern California Chapter</td>
<td>October 8, 2015</td>
<td>Educational Seminar • San Francisco, CA</td>
</tr>
<tr>
<td></td>
<td>October 15, 2015</td>
<td>PLUS Foundation Golf Outing • San Francisco, CA</td>
</tr>
<tr>
<td></td>
<td>December 2, 2015</td>
<td>Holiday Party • San Francisco, CA</td>
</tr>
<tr>
<td>Northwest Chapter</td>
<td>December 2, 2015</td>
<td>Educational Seminar w/ IIABKC • Seattle, WA</td>
</tr>
<tr>
<td>Southeast Chapter</td>
<td>October 8, 2015</td>
<td>Networking Reception • Nashville, TN</td>
</tr>
<tr>
<td></td>
<td>October 19, 2015</td>
<td>PLUS Foundation Golf Outing • Milton, GA</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>Sponsor Appreciation and Networking Reception • Atlanta, GA</td>
</tr>
<tr>
<td></td>
<td>December 2015</td>
<td>Sponsor Appreciation and Networking Reception • Birmingham, AL</td>
</tr>
<tr>
<td>Southern California Chapter</td>
<td>September 24, 2015</td>
<td>Educational Seminar • Los Angeles, CA</td>
</tr>
<tr>
<td></td>
<td>December 10, 2015</td>
<td>Educational Seminar • Los Angeles, CA</td>
</tr>
<tr>
<td>Southwest Chapter</td>
<td>November 2015</td>
<td>Educational Seminar • Las Vegas, NV</td>
</tr>
<tr>
<td></td>
<td>October 1, 2015</td>
<td>Educational Seminar • Scottsdale, AZ</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>Networking Reception • Scottsdale, AZ</td>
</tr>
<tr>
<td>Southern California Chapter</td>
<td>October 8, 2015</td>
<td>Educational Seminar • Los Angeles, CA</td>
</tr>
<tr>
<td></td>
<td>October 19, 2015</td>
<td>PLUS Foundation Golf Outing • Milton, GA</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>Sponsor Appreciation and Networking Reception • Atlanta, GA</td>
</tr>
<tr>
<td></td>
<td>December 2015</td>
<td>Sponsor Appreciation and Networking Reception • Birmingham, AL</td>
</tr>
<tr>
<td>Southeast Chapter</td>
<td>November 2015</td>
<td>Educational Seminar • Las Vegas, NV</td>
</tr>
<tr>
<td></td>
<td>October 1, 2015</td>
<td>Educational Seminar • Scottsdale, AZ</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>Networking Reception • Scottsdale, AZ</td>
</tr>
<tr>
<td>Southern California Chapter</td>
<td>October 8, 2015</td>
<td>Educational Seminar • Los Angeles, CA</td>
</tr>
<tr>
<td></td>
<td>October 19, 2015</td>
<td>PLUS Foundation Golf Outing • Milton, GA</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>Sponsor Appreciation and Networking Reception • Atlanta, GA</td>
</tr>
<tr>
<td></td>
<td>December 2015</td>
<td>Sponsor Appreciation and Networking Reception • Birmingham, AL</td>
</tr>
<tr>
<td>Southwest Chapter</td>
<td>November 2015</td>
<td>Educational Seminar • Las Vegas, NV</td>
</tr>
<tr>
<td></td>
<td>October 1, 2015</td>
<td>Educational Seminar • Scottsdale, AZ</td>
</tr>
<tr>
<td></td>
<td>November 2015</td>
<td>Networking Reception • Scottsdale, AZ</td>
</tr>
</tbody>
</table>

International Events

2015 PLUS Conference
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 11-13, 2015</td>
<td>Hilton Anatole • Dallas, TX</td>
</tr>
</tbody>
</table>

2016 MedPL/PRS Symposia
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 20-21, 2016</td>
<td>Chicago, IL</td>
</tr>
</tbody>
</table>

2016 D&O Symposium
<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 3-4, 2016</td>
<td>Marriott Marquis • New York, NY</td>
</tr>
</tbody>
</table>

THANK YOU, DIAMOND SPONSORS!

The mission of the Professional Liability Underwriting Society is to be the global community for the professional liability insurance industry by providing essential knowledge, thought leadership and career development opportunities.

As a nonprofit organization that provides industry information, it is the policy of PLUS to strictly adhere to all applicable laws and regulations, including antitrust laws. The PLUS Journal is available free of charge to members of the Professional Liability Underwriting Society. Statements of fact and opinion in this publication are the responsibility of the authors alone and do not imply an opinion on the part of the members, trustees, or staff of PLUS. The PLUS Journal is protected by state and federal copyright law and its contents may not be reproduced without written permission.