



March 2016

Five Challenges Facing Employers in the Health Care Industry

Employers in the health care industry are facing a number of looming threats. Workplace violence is one of the most serious occupational hazards facing health care workers, while cyber-attacks pose a significant threat to the sensitive data hosted by health care employers. Other areas of vulnerability concern union organizing activity and, in light of the expanded definition of “joint employment” by the U.S. Department of Labor (“DOL”), the risk of health care employers being considered joint employers. Finally, to fortify against class action risk, employers in the home health care industry must carefully navigate the compliance challenges associated with criminal background checks.

For the latest employment, labor, and workforce management news and insights concerning the health care and life sciences industry, please visit and subscribe to Epstein Becker Green’s [Health Employment and Labor Law blog](#).

In this month’s *Take Five*, we will address these sources of vulnerability and what health care employers need to know to minimize these risks:

- 1. Cal/OSHA Proposes Extensive Regulations to Address Workplace Violence in Health Care Settings—Will Federal OSHA Follow Suit?**
 - 2. Relaxed Legal Ransomware: Give Me Back My Files!**
 - 3. Don’t Overlook Labor Relations Issues in Transactions Involving Health Care Facilities**
 - 4. DOL Expands Its Reach into the Private Sector by Broadening the Definition of “Joint Employment”**
 - 5. The Home Health Care Industry Faces an Escalating Number of Criminal Background Check Laws and Requirements**
-

1. Cal/OSHA Proposes Extensive Regulations to Address Workplace Violence in Health Care Settings—Will Federal OSHA Follow Suit?

By Valerie Butera

The California Division of Occupational Safety and Health, better known as “Cal/OSHA,” recently proposed sweeping regulations addressing workplace violence in health care settings. These far-reaching regulations cover health care workers in a broad range of health care settings, such as outpatient medical offices and clinics, home health care and home-based hospice, emergency medical services, mobile clinics and dispensing operations, drug treatment programs, medical outreach services, and other off-site operations, including retail outlets that provide health care services. Cal/OSHA, known for developing demanding workplace safety regulations, drafted the proposed regulations to implement the Healthcare Workplace Violence Prevention Act (SB 1299), signed by Governor Jerry Brown in 2014. The comment period on the proposed regulations closed on December 17, 2015, but the final regulations have not yet been filed with the Secretary of State.

Meanwhile, there has been a flurry of activity by the federal Occupational Safety and Health Administration (“OSHA”) regarding workplace violence in health care settings. In the past several months OSHA has published a massive overhaul of its [Guidelines for Preventing Workplace Violence for Health Care and Social Service Workers](#) and added a page on its website providing more substantial guidance to aid employers and employees in preventing and responding to workplace violence in health care. The agency has not gone so far as proposing a regulation applicable to workplace violence in health care settings. Although OSHA has issued a number of citations to health care employers with allegedly inadequate workplace violence prevention programs, the agency has used its catch-all provision, the General Duty Clause, when issuing these citations.

All health care employers—regardless of location—should pay careful attention to Cal/OSHA’s proposed regulations as OSHA may refer to them for additional guidance if the agency promulgates federal regulations regarding workplace violence in health care settings.

Overview of the Cal/OSHA Regulations

The proposed regulations broadly define workplace violence as “any act of violence or threat of violence that occurs at the work site” and require employers to “establish, implement and maintain an effective workplace violence prevention plan (Plan) that is in effect at all times in every unit, service, and operation.” The Plan contains a demanding list of requirements, including:

- maintaining sufficient staff (including security personnel) who can keep order in the facility and respond to workplace violence incidents in a timely manner;
- removing or controlling furnishings and other objects that may be used as improvised weapons;

- installing an alarm system (or other effective means) by which employees can summon security and other personnel to respond to an actual or potential workplace violence emergency;
- establishing a response plan for actual or potential workplace violence emergencies that includes obtaining help from facility security or law enforcement agencies, as appropriate; and
- configuring facility spaces so that employee access to doors and alarm systems cannot be impeded.

The proposed regulations mandate that employers provide effective training to all employees, including temporary employees, working in the facility, unit, service, or operation. The training must be provided initially to all employees. Employees performing patient contact activities—and those employees’ supervisors—must be provided refresher training at least annually.

What Does All This Mean for Health Care Employers?

While these regulations are applicable only to health care employers in California, health care employers in all states should strongly consider incorporating the concepts of the proposed Cal/OSHA regulations as well as guidance provided by OSHA for creating effective workplace violence prevention programs in health care settings. The generally positive reception to the Cal/OSHA proposed regulations from health care providers could put pressure on OSHA to develop federal regulations incorporating similar standards.

Even if OSHA does not implement workplace violence prevention regulations, health care employers regulated by OSHA will continue to face liability under the General Duty Clause if their workplace violence prevention programs are deemed inadequate to ensure employee safety.

2. Relaxed Legal Ransomware: Give Me Back My Files!

By Adam C. Solander, Adam S. Forman, and Nathaniel M. Glasser

If Ron Howard were to remake his 1996 film *Ransom* today, instead of Mel Gibson passionately screaming, “Give me back my son!” in response to the kidnapper’s demands, he very well could have Gibson scream, “Give me back my files!” in response to a cybercriminal’s demands for ransomware. What is “ransomware”? Assume you are reading email on your personal computer, tablet, or smartphone and you click on an attachment from an unfamiliar source. Within seconds, your device is encrypted and you are locked out of your applications and files. You may have unwittingly fallen victim to a cybercriminal’s trap. Unless you provide payment in a certain amount of time for the decryption key to unlock the device, your personal information will be gone forever.

This form of cyber-attack—known colloquially as a “ransomware” attack, in which a cybercriminal unleashes malware on a company’s computing infrastructure and blackmails the company for access to its own systems—is on the rise. There are a number of different versions of this attack, but common forms include Cryptolocker and

Cyrtowall. A recent report by Intel Corp.'s McAfee Labs predicts that ransomware attacks in 2016 will only continue to grow in number and sophistication.¹

Ransomware's Impact on the Health Care Industry

Health care organizations, in particular, are susceptible to ransomware attacks because their employees are public facing and it may be part of their jobs to open emails from unknown sources. Further, because the health care industry lags behind other regulated industries in terms cybersecurity, employees may not be trained to spot fraudulent messages, and their networks may not be configured to stop the infection before it reaches the company's file system.

For health care organizations, the stakes are extremely high. A hospital subject to a ransomware attack could lose access to certain computer systems, preventing it from exchanging electronic communications regarding the care of its patients. Ultimately, the hospital might have no choice but to pay tens of thousands of dollars in ransom to obtain the decryption key and regain access to its systems and administrative functions. Losing access to its electronic medical record system for even one day, let alone multiple days, could also harm a hospital's reputation.

Equally troubling is the prospect that a health care organization subject to a ransomware attack learns that its patient protected health information ("PHI") and/or employee personally identifiable information ("PII") was accessed by the hackers. Failure to take adequate steps to protect this information can lead to legal liability. Health care organizations that handle PHI are required by the Health Insurance Portability and Accountability Act ("HIPAA") to adopt administrative, technical, and physical safeguards to protect the confidentiality of PHI. In addition, various state and federal laws establish affirmative duties of employers to protect non-HIPAA-covered sensitive information in a secure manner. Finally, as illustrated by the cyber-attack on Sony Pictures Entertainment,² employers may be susceptible to negligence and state law statutory claims by employees whose PII may be stolen or accessed as part of these attacks.

In the wake of these high-profile ransomware attacks, health care organizations should take a series of steps to protect their patients, customers, employees, and corporate information. As an initial matter, companies should conduct a risk assessment and penetration test to determine their network's vulnerabilities and ensure proper network segmentation is in place to isolate an infection if it occurs. Such review allows businesses to identify and address their most pressing needs before these vulnerabilities can be exploited by cybercriminals and to contain the infection when it does occur.

¹ McAfee Labs, *2016 Threat Predictions*, available at <http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf>.

² *Corona v. Sony Pictures Entertainment Inc.*, C.D. Cal., No. 2:14-cv-9600.

What Should Your Business Do in the Face of Ransomware?

Because ransomware attacks leave companies unable to access their systems, businesses should implement comprehensive and routine procedures to back up important, confidential, and sensitive information. That way, even if ransomware leaves the systems themselves inoperative for a period of time, such an attack will not completely cripple a company's ability to continue doing business and serving its patients and/or customers.

Simple administrative and physical safeguards also can aid companies in preventing and limiting the impact of ransomware attacks. Employees should be granted access to workstations, electronic media, and the network only to the extent necessary to perform their jobs or as otherwise permitted by law. Further, because ransomware is generally initiated by an end user, companies should conduct phishing training so that employees are in a better position to spot fraudulent messages that could contain malware.

In the event of a ransomware or other cyber-attack, companies should contact law enforcement and appropriate experts in the field to formulate an immediate, but reasoned, response to the attack. A number of states have enacted legislation subjecting victims of cyber-attacks to various disclosure requirements, and any victims should be familiar with their duties under applicable law.

3. Don't Overlook Labor Relations Issues in Transactions Involving Health Care Facilities

By Michael F. McGahan and Jonathan K. Hoerner

Before entering into a change-of-ownership transaction, a joint venture, or similar transactions involving health care facilities, the parties frequently perform thorough due diligence on health care regulatory matters. Parties to such transactions should also recognize the importance of a due diligence review of labor relations issues. A thorough and coordinated review of such issues can help limit the risk of post-transaction labor surprises that can have significant financial and operational implications for health care entities—even those currently without any unionized employees.

Looking Beneath the Surface to Anticipate Potential Post-Transaction Labor Issues in Nonunion Workforces

The time before and during a change of ownership or corporate structure can be a period of great uncertainty for employees of a health care entity. Employees may worry not only about whether their compensation, benefits, and work environment will change but also about whether they will still have a job once the change of ownership is completed. This period of uncertainty can be ripe for union organizing activities in a nonunion workforce, or cause interest in an expansion of union representation where part of a workforce is already represented. There have been reports of employees organizing shortly after completed transactions involving health care entities. Further,

the ruling by the National Labor Relations Board (“NLRB”) in *Specialty Healthcare*³ allowing union organization in “micro units” in health care institutions (other than acute care hospitals) will make organizing easier for unions.

To begin with, the due diligence effort must address whether there are any ongoing attempts to organize the workforce, such as NLRB representation proceedings, direct demands for recognition from unions, or evidence of organizing or card-signing campaigns. The review should include an overall audit for vulnerabilities to union organizing efforts, analyze whether the institution is paying competitive wages and benefits, and examine records of employee complaints about workplace issues. In addition, the review should confirm proper compliance with the many laws governing employment (such as wage and hour laws, the Family Medical Leave Act, laws governing discrimination and harassment, and similar laws on a federal, state and, increasingly, local level) because poor compliance with those laws could be used by unions as a basis for organizing activities.

What to Look for When the Workforce Is Already Organized

Where the workforce is represented either in whole or in part by a union, the collective bargaining agreements (“CBAs”) must be reviewed. The CBAs will disclose not just current wages and benefits but also scheduled increases in wages and employer contributions to pension and health care funds. A due diligence review should identify the expiration date of CBAs, which will trigger a new round of bargaining.

When a CBA indicates that participation in multiemployer pension or health funds is required, the review should be expanded to include the financial health of the plans and the benefits provided. In particular, multiemployer pension plans should be critically examined under the Pension Protection Act and the Multiemployer Pension Reform Act. Severely underfunded plans will likely have adopted rehabilitation plans that require hefty increases in employer contributions each year. They also carry the potential for massive withdrawal liability under the Employee Retirement Income Security Act of 1974 (“ERISA”) if the employer ceases contributions to the fund or the fund suffers a “mass withdrawal” of employers. Parties also need to examine whether a withdrawal has already occurred and withdrawal liability incurred, or whether the transaction itself will trigger withdrawal liability. Several recent federal court decisions have imposed withdrawal liabilities on successor employers in asset purchase agreements.⁴

Employee health plans, particularly multiemployer health plans, can have potential hidden liabilities for an acquiring or partnering health care entity. These plans need to be carefully evaluated for compliance with the many mandates of the Affordable Care Act. Past increases in employer contributions or costs should be reviewed as part of projecting future health coverage costs for the entity.

The CBAs should be reviewed by labor counsel to determine the applicability of any successorship language that could require the acquiring entity to recognize the union

³ 357 NLRB 934 (2011).

⁴ See, e.g. *Resilient Floor Covering Trust Fund v. Michael's Floor Covering, Inc.*, Case No. 12-17675 (9th Cir. Sept. 11, 2015).

and honor existing CBAs, or purport to require that the union be recognized by, and the CBA applied to, any new or acquired facilities. It is also important to identify “neutrality” clauses, which require that the employer not oppose any union organizing efforts in unrepresented job classes or at other locations owned or operated by the employer.

The interactions and working relationship between the entity and the unions representing the employees needs to be carefully reviewed. A review of past and pending unfair labor practice charges, grievances, and arbitration proceedings should be made to evaluate risk of adverse decisions. Pending grievances and arbitrations have the potential for new interpretations of existing CBA clauses and practices that may carry with them increases in operating costs. Further, liability for prior unfair labor practices can be imposed on successor employers.

Labor relations issues and terms of CBAs can have long-standing effects on future operations and significant financial implications both in the present and well into the future. An investment in labor relations diligence before entering into a transaction may prevent costly workforce surprises after the transaction is completed.

4. DOL Expands Its Reach into the Private Sector by Broadening the Definition of “Joint Employment”

By Nathaniel M. Glasser and Jamie F. Friedman

Health care employers should be cognizant of regulators’ continuing focus on joint employment issues, from the increasingly common scenario in which businesses rely on staffing agencies to supplement their workforce, to situations in which businesses use a common pool of workers. Late last year, we highlighted the NLRB’s new test for establishing joint-employer status under the National Labor Relations Act (“NLRA”), which affects staffing arrangements and third-party service contracts commonly used in the [health care industry by broadening the test for joint employment](#). On January 20, 2016, the DOL’s Wage and Hour Division issued its Administrator’s Interpretation No. 2016-1 (“AI”), which warns that the DOL will closely monitor employers’ compliance with the Fair Labor Standards Act (“FLSA”) and Seasonal Agricultural Worker Protection Act (“MSPA”).

The DOL identifies two types of joint employment: horizontal joint employment and vertical joint employment, both of which are common arrangements within the health care industry. Horizontal joint employment occurs when a worker has employment relationships with two entities that are sufficiently affiliated such that they jointly employ the worker. Vertical joint employment exists when an employee of one company is, with respect to the work for that company, also economically dependent on another company.

The AI’s Impact on the Health Care Industry

Health care employers have long known that they might be considered joint employers with their temporary workers provided by health care staffing agencies. Over 15 years ago, the [Equal Employment Opportunity Commission \(“EEOC”\) advised](#) health care providers that, for purposes of liability under the Americans with Disabilities Act, they

may be considered a joint employer of temporary nurses or other workers hired through a staffing firm.

In 2008, the U.S. Court of Appeals for the Second Circuit incorporated this concept of joint employment into the wage and hour sphere. In *Barfield v. N.Y. City Health & Hosps. Corp.*, health care employers were put on notice that they could be considered joint employers when using staffing agencies to provide workers who are economically dependent on the hospital.⁵

The employment relationship at issue in *Barfield* is cited by the AI as an example of vertical joint employment, which is exemplified by the use of staffing agencies and other third parties to supplement a company's workforce. Vertical employment focuses on whether the worker, who is placed at a company or hospital by a staffing agency with which the company or hospital has contracted for services, can be considered an employee of both the staffing agency and the company or hospital. Health care employers using contracted workforces must ensure that these workers are properly classified according to the economic reality of their position within the company or risk the negative consequences of a DOL audit.

Employers in the health care industry must also consider the classification of a worker who provides services for more than one company where the companies are sufficiently related so as to be considered a joint employer. To highlight this scenario—known as “horizontal joint employment”—the AI provides the example of a nurse who works for two hospitals that are considered joint employers. In that situation, both hospitals are jointly and severally liable for compliance with the FLSA, including paying overtime compensation for all hours worked over 40 during the workweek, even if the nurse works fewer than 40 hours per week for each hospital separately.

The DOL unambiguously interprets the test for joint employment under the FLSA more broadly than the test under the NLRA and other labor statutes. The DOL's position on joint employment, however, likely will have consequences that extend beyond the FLSA.⁶

The AI further makes clear that the DOL will analyze potential joint employment under both the vertical and horizontal axes; in so doing, joint employment will be easier to find. The AI explicitly cautions that its new approach to joint employment will allow it to collect back wages from a larger “deep pocket” entity, which will now be considered the joint employer with a smaller entity.

How Should Health Care Employers Respond to the AI?

Employers should take preventative measures to stay ahead of the DOL. Employers utilizing contracted workforces should make sure to have in place written agreements that address the DOL's definition of “joint employment” and, where possible, contain provisions that define a true independent contractor relationship.

⁵ *Barfield v. N.Y. City Health & Hosps. Corp.*, 537 F.3d 132, 143-49 (2d Cir. 2008).

⁶ For a discussion of the impact of this AI on H-1B dependent employers, please see our colleague Jang Im's recent article, “Steps for Avoiding Unexpected Joint Employment Liability,” *Law360* (Feb. 16, 2016).

Employers—especially those in the process of joining or merging with a network, or who are entering a business relationship with a substantially smaller entity—also are advised to conduct an audit to ensure compliance with the broadened definition of “joint employment.” As joint employers are joint and severally liable for compliance with the FLSA (and subject to a longer statute of limitations period when the misclassification is “willful”), it is imperative that health care companies properly classify employees and properly document independent contractors.

5. The Home Health Care Industry Faces an Escalating Number of Criminal Background Check Laws and Requirements

By Denise Merna Dadika

Home health care is one of the fastest growing industries in the United States. As the population continues to age, the demand for home health care is expected to increase dramatically. One of the several challenges facing the home health care industry is selecting qualified and trustworthy individuals to provide unsupervised patient care to a vulnerable population. Conducting criminal background checks on prospective employees is one practice that employers in the home health care industry should implement to select a qualified and trustworthy workforce, but conducting background checks presents its own challenges, given the number of federal, state, and local laws, as well EEOC guidance, that employers must comply with when conducting background checks.

State Requirements

There are no federal laws or regulations that require home health agencies (“HHAs”) to conduct criminal background checks or disqualify applicants from employment based on the results.⁷ There are, however, 41 states that require HHAs to conduct criminal background checks. The requirements in those 41 states vary widely, including when the background check must be completed, what sources of information must be checked, which positions require background checks, and which convictions, if any, result in disqualification from employment.

In addition, the Affordable Care Act established the framework for a Nationwide Background Check Program, which provides grants to states to implement statewide background checks on all prospective direct patient access employees of long-term care facilities and providers, including HHAs. CMS has awarded more than \$50 million

⁷ The Office of Inspector General (“OIG”) has authority to exclude individuals and health care entities from federally funded health care programs based on conviction of certain crimes. Excluded individuals are posted to the OIG’s List of Excluded Individuals and Entities. Health care entities are required to regularly check the list to avoid hiring excluded individuals or billing for services rendered by excluded individuals but are not required to independently conduct background checks.

to 26 states to design comprehensive background check programs for direct patient access employees.⁸

EEOC Guidance

In addition, HHAs should be mindful of the EEOC's position on the use of criminal history in hiring decisions. Over the past few years, the EEOC has taken an aggressive stance on employers' use of criminal background checks because the agency believes that such background checks disproportionately affect minorities. In 2012, the agency issued updated guidance cautioning employers that hiring decisions based on criminal history should be job-related and consistent with business necessity. The guidance directs employers to conduct individualized assessments for applicants excluded by a criminal background check by considering the following factors: the nature and gravity of the offense or conduct; the time that has passed since the offense, conduct, and/or completion of the sentence; and the nature of the job held or sought.

Since issuing its guidance, the EEOC has filed numerous disparate impact discrimination lawsuits challenging criminal background check policies and practices. While the EEOC has suffered a number of defeats, it recently entered into a \$1.6 million settlement with BMW⁹ concerning the company's background check practices. Given the EEOC's recent success, it likely will continue to challenge employers' use of criminal background checks that it believes has a disparate impact on minority groups.

Thus, HHAs should proceed with caution when making ultimate employment decisions based on the results of criminal background checks. For those criminal convictions that do not result in automatic disqualification from employment per applicable state laws, HHAs should consider conducting an individualized assessment prior to excluding an applicant based on criminal history. HHAs should also consider carefully limiting the circumstances in which an applicant may be automatically excluded from employment based on certain convictions in light of EEOC's guidance.

“Ban the Box” Legislation

HHAs also must be aware of the number of states, counties, and cities that have passed ban-the-box legislation limiting the use of criminal records in hiring. There are currently seven states (Hawaii, Illinois, Massachusetts, Minnesota, New Jersey, Oregon, and Rhode Island) and more than 100 counties and cities (including Baltimore, New York City, Newark, Philadelphia, San Francisco, Seattle, and Washington, DC) that have enacted legislation covering private employers. Generally, ban-the-box legislation restricts the timing of when an employer may inquire about an applicant's criminal history (e.g., after the first interview or after a conditional offer has been made), but some of the laws (e.g., in New York City and Philadelphia) require employers to

⁸ See Centers for Medicare & Medicaid Services, CMS National Background Check Program, <https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/BackgroundCheck.html>.

⁹ *EEOC v. BMW Manufacturing Co., LLC*, D.S.C., No. 7:13-cv-1583.

consider a list of factors before disqualifying an applicant based on criminal history. HHAs should determine whether they are subject to ban-the-box legislation, as certain laws specifically exclude HHAs from coverage (e.g., Washington, DC's law does not apply to employers that provide "direct care to minors or vulnerable adults"), and comply with the applicable timing limitations, as well as any other requirements, when conducting criminal background checks.

Fair Credit Reporting Act

Although no federal laws require HHAs to conduct criminal background checks, if an employer uses a third party to prepare its background reports, it must comply with the federal Fair Credit Reporting Act ("FCRA"), as well as any state background check laws. FCRA imposes a number of procedural requirements in connection with the background check process. Within the last two years, the number of FCRA class actions has skyrocketed. These litigations focus on the employers' compliance with disclosure requirements; specifically, whether employers have violated FCRA's standalone disclosure requirement by including the disclosure in the job application¹⁰ or by incorporating at-will or EEO language in the disclosure document.¹¹ In addition, class actions also have questioned the adverse action requirements, which require the employer to follow a two-step process of sending a pre-adverse action letter followed by an adverse action letter if it intends to take an "adverse action."¹²

The recent class actions demonstrate that compliance with FCRA is critical when HHAs make their hiring decisions. Given the hyper-technical FCRA requirements, HHAs should consider arranging for a privileged review of background check forms, notices, disclosures, and templates.

Carefully navigating the various federal, state, and local laws, as well as the EEOC's guidance, when conducting background checks may prove challenging for HHAs, but it is a critical step in hiring a qualified workforce in this industry.

¹⁰ *Ford v. CEC Entertainment, Inc.*, N.D. Cal., No. 14-cv-01420; *Camacho v. ESA Management LLC*, S.D. Cal., No. 14-cv-01089; *Castro v. Michael Stores*, N.D. Tex., No. 15-cv-00276.

¹¹ *Mack v. Panera*, S.D. Fla., No. 14-cv-61672.

¹² *Jones v. Halstead Mgmt. Co., LLC*, S.D.N.Y., No. 14-cv-03125; *Ramos v. Genesis Healthcare, LLC*, E.D.Pa., No. 15-cv-00052.

For additional information about the issues discussed above, please contact the Epstein Becker Green attorney who regularly handles your legal matters or any of the authors of this *Take 5*:

Nathaniel M. Glasser
Washington, DC
202-861-1863
nglasser@ebglaw.com

Adam C. Solander
Washington, DC
202/861-1884
asolander@ebglaw.com

Adam S. Forman
Chicago
312-499-1468
aforman@ebglaw.com

Valerie Butera
Washington, DC
202-861-5325
vbutera@ebglaw.com

Michael F. McGahan
New York
212-351-3768
mmcgahan@ebglaw.com

Denise Merna Dadika
Newark
973-639-8294
ddadika@ebglaw.com

Jonathan K. Hoerner
Washington, DC
202-861-1826
jhoerner@ebglaw.com

Jamie F. Friedman
New York
212-351-3744
jfriedman@ebglaw.com

This document has been provided for informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

About Epstein Becker Green

Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labor, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the U.S. and supporting clients in the U.S. and abroad, the firm's attorneys are committed to uncompromising client service and legal excellence. For more information, visit www.ebglaw.com

© 2016 Epstein Becker & Green, P.C.

Attorney Advertising