ARTICLE 06: PART 1

REDUCING RISK IN FIELD SALES OPERATIONS

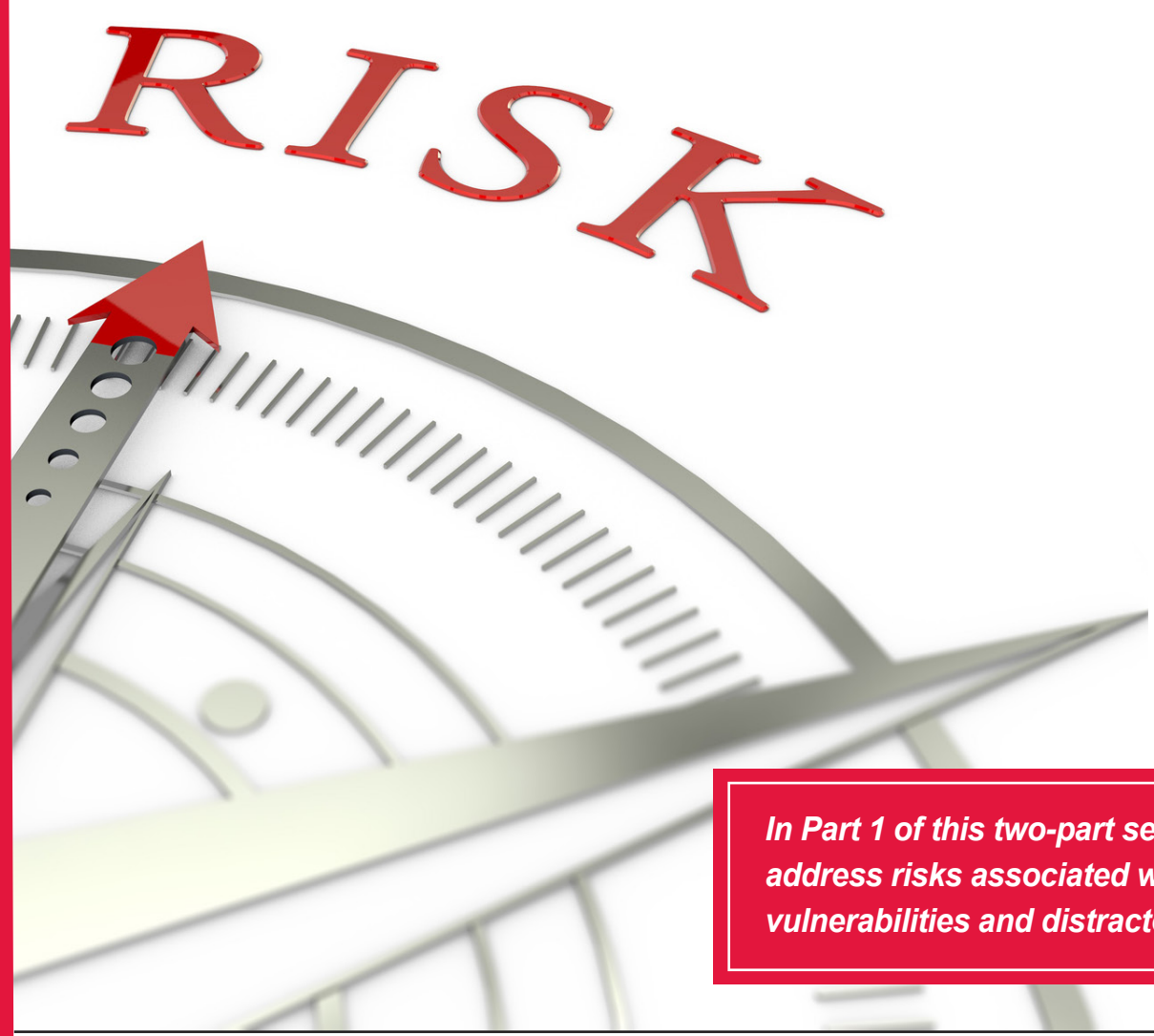
By Kristin Berger Parker

In This Article:

MEDICAL ALLEY ASSOCIATION

STINSON LEONARD STREET

Reducing Risk in Your Field Sales Operation — Part 1



Field sales employees are critical to distribution and ultimately achieving revenue goals. However, the inability of employers in the supply chain to directly supervise field sales employees creates underappreciated risks which may negatively impact profitability.

In some cases, liability may be directly caused by the acts or omissions of the employee. In other cases, field sales employees may be exposed to risks by third parties that are not fully visible to or within the control of employers.

Careful evaluation of these risks and implementation of policies, procedures and employee training can help ensure that your field sales team remains an asset and not a liability.

In Part 1 of this two-part series, we will address risks associated with electronic vulnerabilities and distracted driving.

Addressing Electronic Vulnerabilities

Electronic devices are ubiquitous in the workplace, and even more so for outside sales employees. Employees live off their email or text messages, and with electronic medical records and tablets becoming more common, a single employee could possess three electronic devices at one time. Employers should be cognizant of the risks of disclosure and design policies to protect competitive and/or other protected information.

Allowing (or requiring) employees to bring their own devices or port their numbers carries competitive risks—e.g., that they will retain the number (and contacts) when they move on to a new employer. Lack of digital rights management on your documents also poses a risk that documents will be forwarded out of your system, potentially for competitive use. Unless employee phones are synched to your systems, monitoring of text messages is difficult or impossible.

HIPAA violations may arise in numerous ways from use of mobile devices:

- Most commonly, employees may communicate protected health information via email or text message without appropriate authorization or encryption.
- Employees who use a single device for work and personal use may make social media posts that disclose location information, images that inadvertently reveal protected health information or other comments that violate HIPAA or state medical privacy laws. Use of a single device for work and personal use may also lead to access of protected information by family members.
- Tablets used to gather medical information from patients or physician clients and which have capabilities to store the information on the device (rather than in the cloud) pose a risk if they are mislaid.

There are several best practices for managing these risks:

Training employees to include minimum necessary information in electronic communications

Device, email and social media modules in HIPAA training

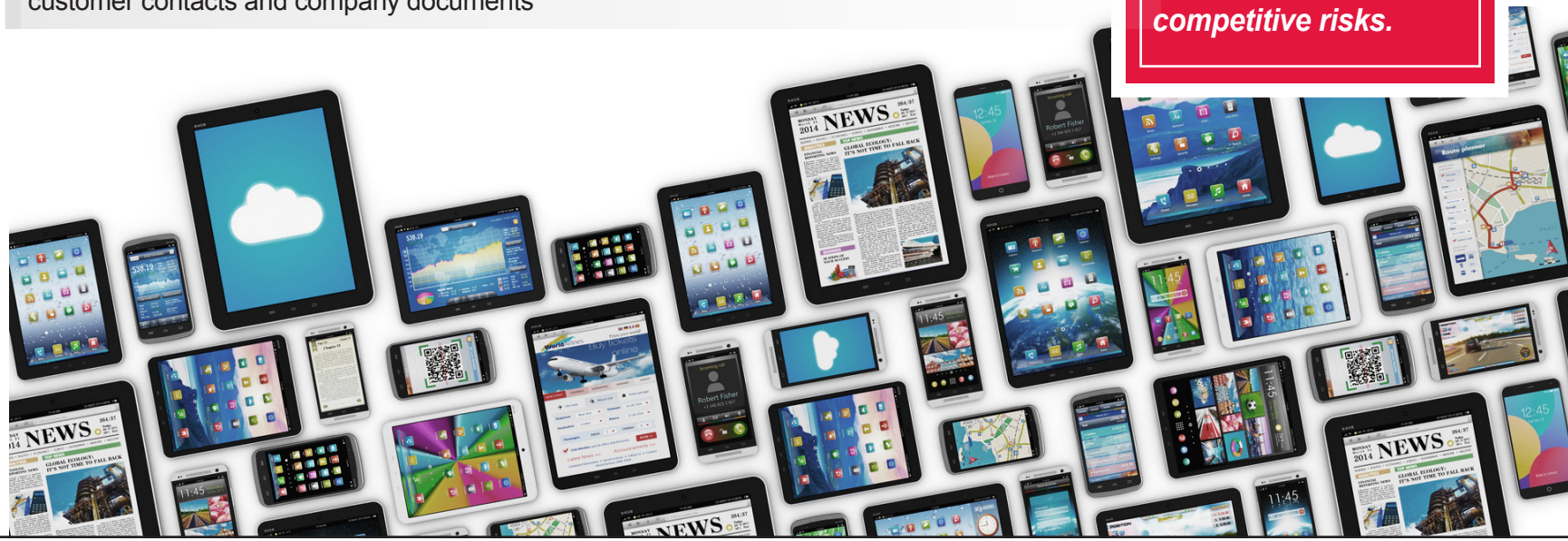
Express provisions regarding confidential, proprietary and other protected information in company-owned and bring-your-own device policies

Implementation of dual-factor authentication for access to company systems

Application of digital rights management on confidential and proprietary documents

Requiring use of apps—which include encryption technologies and that can be remotely wiped from the phone or other device—for access to email systems, customer contacts and company documents

Allowing or requiring employees to bring their own devices to work or to port their mobile phone numbers to work-issued devices carries several competitive risks.



Driven to Distraction

Another risk of electronic device use is more visceral: distracted driving can lead to serious injury or death of employees and third parties. Such concerns should be top of mind when managing a workforce that is both necessarily mobile and responsive to customer communications.

Many sales employees, as well as company executives, use electronic devices to review and respond to work-related voice and written communications during the workday and business travel. These devices may also be used for business functions such as placing orders, managing customer relations and route planning.

At a minimum, company policies should require compliance with state laws regarding use of electronic devices. However, these laws vary between jurisdictions, which can lead to a patchwork of different practices. Forty-seven states prohibit text messaging for all drivers. Fifteen states prohibit use of handheld cell phones while driving, although the strictness of the ban varies. And some states permit holding the phone to dial or to use the GPS feature.

Additionally, no state completely prohibits use of hands-free cellular devices while driving. Citing the cognitive load of such communications as a significant risk factor in motor vehicle crashes, the National Transportation Safety Board and various safety organizations recommend that employers implement total cell phone ban policies, which prohibit use of all handheld and hands-free devices in employer-vehicles, on employer time and with respect to work-related communications.

Distracted driving should be top of mind when managing a workforce that is both mobile and responsive to customer communications.

Risks related to use of electronic devices while driving include:

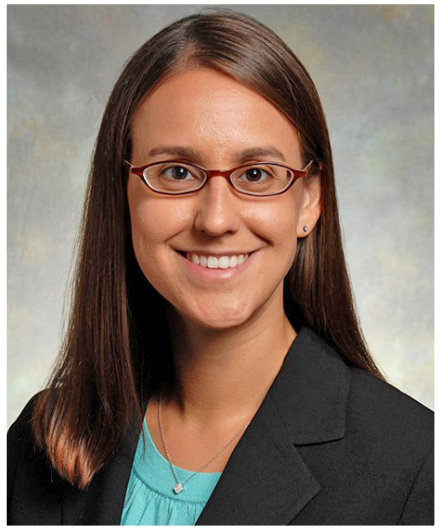
- Damage to company property
- Injury to employees, resulting in potential workers' compensation claims
- Negative publicity
- Potential company liability for damage or personal injury to third parties, if the employee is acting within the scope of his or her employment at the time of a crash

Customized Risk Solutions for Your Company

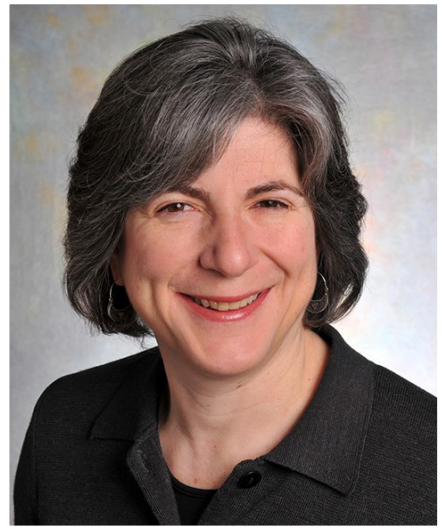
To learn how you can build policy safeguards against the risks of distracted driving and electronic vulnerabilities, contact one of the attorneys noted on the right.

Also, look for Part 2 of this series in February. That article will evaluate bloodborne pathogen risks and reveal how you can avoid OSHA retaliation claims.

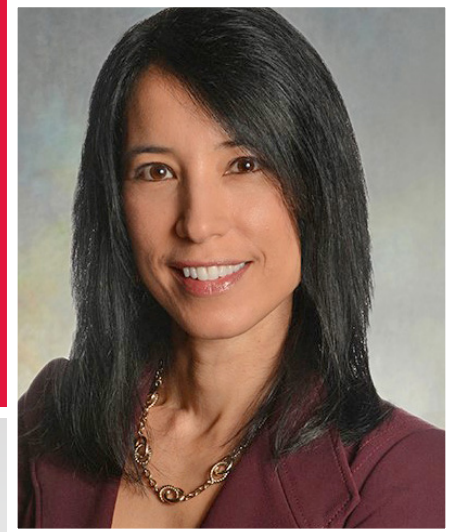
Supply Chain Series Contributors



Kristin Berger Parker, an attorney at Stinson Leonard Street LLP, represents employers in all aspects of the employment relationship. She partners with employers in a variety of industries, including health care and technology, to advance their business goals through workforce policies and strategies, while identifying and minimizing risk.



Sheva Sanders practices health law at Stinson Leonard Street LLP. She advises healthcare, managed care, medical device, pharmaceutical, life sciences and PBM clients on complex regulatory issues including fraud and abuse, compliance, reimbursement and transactional matters. She is a frequent teacher, speaker and writer on topics related to health law and health policy.



Tricia Kaufman, an attorney at Stinson Leonard Street LLP, focuses her practice on the life sciences industry. She counsels medical device and pharmaceutical manufacturers and their vendors, drug compounding outsourcing facilities, healthcare providers, GPOs and others on issues relating to FDA regulations and healthcare compliance laws.