EPSTEIN
BECKER
GREEN

Return-to-Work

Top Privacy and Cybersecurity Considerations for Retail Employers

NRF
National
Retail
Federation

Complying with Data Security and Worker Privacy Laws

☐ Ensure that any policies and procedures created to address health, safety, and productivity concerns will be compliant with state, federal, and international data security/privacy laws.

☐ Inform workers of any new or sensitive information being collected from them (e.g., in screening or testing procedures or in connection with a vaccination policy), how it will be used, and how it will be stored to ensure notice is in compliance with applicable law (e.g., the California Consumer Privacy Act (“CCPA”), the General Data Protection Regulation (“GDPR”), or other relevant state laws).

☐ Ensure the maintenance of worker privacy rules (including those relating to health and medical information) under:

» the Americans with Disabilities Act, the Genetic Information Nondiscrimination Act, and the antidiscrimination laws that are enforced by the Equal Employment Opportunity Commission (“EEOC”);
» the Health Insurance Portability and Accountability Act (“HIPAA”);
» laws restricting the use of biometrics (e.g., carefully consider the legal issues concerning the use of facial recognition software, or wristwatches or mobile apps that track workers’ locations or check their temperatures); and
» applicable state laws (the CCPA and the Illinois Transparency and Privacy Act) as well as certain international laws, including the GDPR.

☐ Implement reasonable cybersecurity and data privacy safeguards to protect personal information under the New York State Stop Hacks and Improve Electronic Data Security Act (or “SHIELD Act”), the CCPA, and other applicable laws.

☐ Provide cybersecurity training to raise awareness of remote and in-person workers to reinforce the practices that help identify vulnerabilities and prevent cyber incidents and breaches before they occur.

Vaccination

☐ Assess whether COVID-19 vaccination policy contemplates data privacy and security concerns.

☐ If requiring proof of vaccination, determine what information is acceptable, how it will be used (including to verify time off), and length of retention.

☐ Ensure proper safekeeping of confidential health information (e.g., health information should not be kept with other general employment records).

☐ If considering using vaccination passports for workforce or customers, ensure compliance with applicable federal, state, or local laws (note that some states are banning the use of vaccination passports in certain circumstances).

Testing/Tracking Workers Returning to the Workplace
(temp scans, social distancing apps, etc.)

☐ Ensure that procedures requiring employees to have temperature taken before reporting to work are compliant with EEOC guidance, including confidentiality requirements, and wage and hour laws.

☐ Are apps or devices to be used accessible to employees with disabilities as, for example, blind or low-vision or hearing-impaired individuals?

☐ Conduct Privacy Impact Assessments to evaluate the sensitivity of the data, identify the controls needed to protect the data, and specify the mitigations needed to reduce the risks associated with the tools used to store the data collected.

☐ If COVID-19 or antibody testing will be provided through an employer-sponsored group health plan, Employee Assistance Program, or onsite medical clinic and shared with the employer, consider any applicable obligations under HIPAA.

☐ Consider whether the implementation of technologies or new policies require bargaining/negotiation with union representatives, where applicable.

Return to Work:

Top Privacy and Cybersecurity Considerations for Retail Employers

Asking Workers to Share Information to Reopen and Maintain a Safe Workplace, and Protecting Worker Information

□ **Comply with EEOC and other regulatory guidance if requesting a doctor's note from workers for reasonable accommodation requests, leaves, or a return to work.**

□ **Comply with EEOC guidance if considering the use of travel and COVID-19 questionnaires, including requesting that workers provide details regarding recent travel and whether they have, or do not have, COVID-19.**

□ **Ensure that all information collected is maintained securely and confidentially (e.g., do not include medical records in an employee's general personnel file).**

Disclosing information

(i.e., to public health officials, etc., if someone tests positive)

□ **Create policies and procedures to govern disclosures made by workers who were exposed to, or tested positive for, COVID-19 to address the following:**

» To whom should exposed or infected workers report this information?

» Whom (other workers or others) should or must employers notify, and what precautions should employers take to ensure that the worker's identity is protected? (Consider CDC, state, and local requirements.)

» What information cannot be released without consent? What information can be released without consent? What information, if any, must be disclosed to public health or governmental entities?

Understanding Cyber Essentials for Preventing Hackers from Exploiting the COVID-19 Crisis

□ **Think in terms of people, information, and machines.**

□ **Develop a written risk assessment and information security plan to include remote workers and protected personally identifiable information.**

□ **Consider implementing multi-factor authentication as the default authentication method for remote user access from the home.**

□ **Consider and address the risks of allowing workers to access organizational resources using company computers/devices vs. personal ("BYOD") computers/devices.**

□ **Consider and address the risk of permitting direct remote access to web-based organizational resources.**

□ **Consider and plan for the most likely threats.**

□ **Plan for remote worker security incidents.**

□ **Have workers sign strong confidentiality and acceptable use agreements, and plan for the termination of remote workers.**

□ **Encrypt laptops and mobile devices containing protected or sensitive information.**

Monitoring Workers Working Remotely
(from invasions of privacy to performance)

□ **If contemplating productivity software (e.g., spyware/surveillance/keystroke logging), consider legal implications:**

- Ensure compliance with the Electronic Communications Privacy Act (including Federal Wiretap Act and Stored Communications Act), state and local social media password protection laws, state data protection laws (e.g., the CCPA), and similar privacy laws.
- Keep an eye out for new laws regulating the monitoring of remote workers (e.g., NY Assembly Bill 60690, seeking to prohibit electronic monitoring of remote employees).
- If monitoring is permissible under executive orders or an applicable state return-to-work plan, be sure to effectively communicate and provide appropriate notice to workers as to what will be monitored and how the monitoring complies with relevant law.
- Be mindful of National Labor Relation Act's prohibition on surveillance of protected concerted activities.

Questions That Employers Should Ask

□ **What information is being collected?**

□ **Why is the information being collected?**

□ **Can the information be lawfully collected in the manner contemplated?**

□ **What technology/tools are being used, and which third parties may have access to the information those tools collect?**

□ **Are the technology/tools and apps to be used accessible to employees with disabilities?**

□ **How will the information be used/disclosed?**

□ **What safeguards are needed to protect this information?**

□ **How long will the information collection continue, and will the information be deleted?**

□ **Will the data be de-identified, and what are the intended secondary uses of such data?**

□ **Has the employer (and/or, as applicable, its group health plan) provided the proper privacy notices?**

□ **Has the employer addressed data privacy and security issues, breach notification procedures, indemnification, and limitation of liability in its (or, as applicable, its group health plan's) service provider agreements?**

□ **Will any technology or procedures require bargaining with represented employees?**

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.