GENERAL GUIDANCE ON LEGAL ISSUES RELATED TO COVID-19 AND PRIVACY AND DATA SECURITY FOR U.S. COMPANIES[1]

MVA COVID-19 Resource Center
04.2020

With the significant recent healthcare, employment and financial services legislation arising out of the COVID-19 pandemic, and the almost daily updates and guidance, the sea-change in privacy and data security law of the past few years seems like a distant memory. There are, however, a number of important privacy and data security issues of which U.S. companies should be aware, particularly in the areas of employment, compliance with security standards, and vendor management. The following shares guidance and insight into common issues that can arise.[2]

EMPLOYEE PRIVACY

COVID-19 presents a host of privacy and data security concerns in the workplace.

- *Taking Employee Temperatures.* The Americans with Disabilities Act (as amended) (ADAAA) limits an employer's right to engage in medical examinations and inquiries. The Equal Employment Opportunity Commission (EEOC), however, has issued guidance recognizing that taking temperatures of employees to screen for potential COVID-19 infection does not violate the ADAAA either because the infection may be so mild as to not constitute a "disability" under the law or because the infection can pose a "direct threat" to the health or safety of others. Additional concerns include potential damages to employees if they are forced to go home after a positive temperature reading. Employers could have a viable defense to temperature reading under the OSHA obligation to create a safe and healthy working environment. Additionally, given the pandemic, employers should be able to show that the temperature reading is job-related and consistent with business necessity and that persons with a temperature above 100.4 may pose a direct threat.

Employers should encourage employees with low-risk exposure to check their own temperature as part of an effort to confirm that the employee is not demonstrating COVID-19 symptoms.

See EEOC Pandemic Guidance, Section III B(7): https://www.eeoc.gov/facts/pandemic_flu.html

See EEOC April 17, 2020 Guidance https://www.eeoc.gov/eeoc/newsroom/wysk/wysk_ada_rehabilitaion_act_coronavirus.cfm

See EEOC Guidance on Questions and Medical Exams: https://www.eeoc.gov/policy/docs/guidance-inquiries.html

- Employers must maintain the confidentiality of employee medical information and medical leave information. The Family and Medical Leave Act and the Americans with Disabilities Act require that employers keep information about an employee's serious health condition and disabilities (respectively) private and disclose only on a need to know basis. For example, the ADA requires information regarding disabilities and accommodations to be maintained in a confidential medical file and to limit access to the information to supervisors, managers, and human resources employees, but only as necessary to assess reasonable accommodations, identify restrictions on work duties, or otherwise engage in the interactive process required by the ADA, first aid and safety personnel if the disability might require emergency treatment, and government officials investigating compliance with the ADA. 42 U.S.C. § 12112(d)(4)(c); 29 C.F.R. § 1630.14(b)-(d). Notably, although employers should inform other employees who worked in close proximity to an employee diagnosed with COVID-19, the FMLA and the ADA do not permit the employer to identify the diagnosed employee by name.
- *Genetic Information.* One theory coming out of medical research into COVID-19 is that certain genetic traits can make a person more susceptible to serious illness if infected by the virus, and conversely, certain other genetic traits may make a person less likely to get sick. As government stay at home orders are lifted and employers try to staff up with a stable workforce, businesses may be tempted to screen workers for these genetic traits. The federal Genetic Information Nondiscrimination Act (GINA), however, generally prohibits taking adverse employment actions based on genetic information.

Further, family medical history is considered "genetic information" under GINA. Employers should be careful about how to ask whether employee family members are symptomatic. Asking "Is anyone in your household exhibiting symptoms of COVID-19 (fever, coughing, difficulty breathing and shortness of breath)" should not be construed as asking about family medical history as intended by GINA.

- *Limitations on Employees Speaking to the Media*. Prohibiting non-supervisory employees (even if not unionized) from speaking to the media about workplace COVID-19 concerns could violate the National Labor Relations Act ("NLRA"). In a November 4, 2016 Advice Memorandum, the NLRB General Counsel confirmed that under Section 7 of the NRLA, "employees have a right to speak publicly about their complaints or concerns with the terms and conditions of employment, including the process, without employer authorization." However, prohibiting non-supervisory employees from sharing confidential information or stating that only an authorized representative can speak on behalf of the employer should not violate Section 7 rights.
- *Prohibitions on Travel*. Many employers prohibited or limited employee business travel to minimize risk of infection by the novel coronavirus. Prohibiting employees from engaging in personal travel or other risky conduct during nonworking hours, however, is trickier. In some states, employers cannot take adverse employment action against employees for lawful use of lawful products (with some exceptions). For example, in North Carolina, employers cannot "discharge or otherwise discriminate against any employee with respect to compensation, terms, conditions, or privileges of employment because the prospective employee or the employee engages in or has engaged in the lawful use of lawful products if the activity occurs off the premises of the employer during nonworking hours and does not adversely affect the

employee's job performance or the person's ability to properly fulfill the responsibilities of the position in question or the safety of other employees." Likewise, Illinois law (820 ILCS 40/9), prohibits employers from gathering or keeping "a record of an employee's associations, political activities, publications, communications or nonemployment activities, unless the employee submits the information in writing or authorizes the employer in writing to keep or gather the information." The prohibition does not apply to conduct that could be reasonably be expected to harm the employer's property, operations or business or cause the employer financial liability. Employers who want to prohibit certain lawful off duty conduct because of the risk of exposure to COVID-19 should carefully consider whether the prohibition falls within an exception to a state lawful use of lawful products law.

- *Geolocation*. Employers are searching for ways to determine which of their employees may have been exposed to the novel coronavirus by an infected co-worker, vendor or member of the public. One tool is GPS tracking of employees through their electronic devices or vehicles. Some states, however, prohibit or limit such tracking without employee consent. Connecticut for example requires notice of monitoring. California law makes it illegal for a person to use an electronic tracking device to determine the movement or location of an individual, unless the person doing the tracking is the owner, lessor or lessee of the vehicle being tracked or unless the individual being tracked has consented. Even in states without such statutes, notice of tracking is important to take away any employee expectation of privacy in his or her movements. Consent, of course, is even better.
- *Social Media Password Protection Laws.* The Families First Coronavirus Response Act (FFCRA) contains two laws (the Emergency Family and Medical Leave Extension Act (EFMLEA) and the Emergency Paid Sick Leave Act (EPSLA)) providing for paid sick leave and expanded family leave. As with other leave, such as the FMLA, there is risk of employee abuse and employers may be tempted to check out an employee's social media to ensure that the employee is in fact quarantined or otherwise meeting the qualifying conditions for the leave. Under the laws of some states, however, employers cannot force employee to provide password to nonpublic portions of social media (or back channels like "friending" a manager). There are some exceptions for investigations, subject to specific requirements. Public portions of social media pages are not covered by these statutes, but employers should be careful. An employer may obtain information about an employee's protected characteristic (such as sexual preference) that may later be used by the employee to claim illegal discrimination if the employee is terminated or subject to some other adverse employment action.
- *HIPAA*. Most employers are not covered entities under HIPAA. However, health plans are covered entities for HIPAA purposes and therefore subject to HIPAA's Privacy and Security Rules just like a health care provider (except for self-administered plans with fewer than 50 participants). The group health plan is considered to be a separate legal entity from the employer or other parties that sponsor the group health plan. Neither employers nor other group health plan sponsors are defined as covered entities under HIPAA. Therefore, the Privacy Rule does not directly regulate employers or other plan sponsors that are not HIPAA covered entities. However, the Privacy Rule does control the conditions under which the group health plan can share protected health information with the employer or plan sponsor when the information is necessary for the plan sponsor to perform certain administrative functions on behalf of the group health plan. Companies with self-insured group health plans need to be aware that information related to an employee's COVID-19 infection or treatment that the employer obtains from or submits to the plan is subject to HIPAA's protections.

- *Telework*. Telework has become a popular option for businesses either trying to increase social distancing of its employees to control COVID-19 infection or to comply with government "stay at home" orders. In addition, telework may be attractive to employers trying to avoid paid leave under the EFMLEA and the EPLSA. Teleworking presents significant data security risks. Employers should not only ensure technical safeguards are in place to protect personally identifiable information, but also should issue teleworking policies to employees to cover data security and privacy issues. Likewise, employees who are using their own data devices to work should sign a BYOD agreement or at the very least acknowledge a BYOD policy. Employers should require employees working from home to follow the company's data security requirements, including using encrypted devices, accessing the company's information and networks through secure connections (ideally VPN), and using dual factor authentication or other secure methods of access. This is particularly true if employees are using their personal devices for work. Employers should require employees to run all software updates so that security patches are up to date. Likewise, employees should keep home router software updated, change default router names and passwords, encrypt their home wireless network, enable logging and enable firewalls. Employers also can prohibit or place additional security requirements on the use of public Wi-Fi for work. Employers can and should, to the extent feasible, prohibit employees from using personal email or texting to conduct company business, and should prohibit employees from creating or storing company or customer documents and information on personal devices or personal cloud data storage sites. Employees using hard copy files should agree to protect the confidentiality of the files and agree to maintain them in a secure location.
- *Phishing and BECs*. Fraudsters are not letting a good pandemic go to waste. Phishing and business email compromises are rampant, and employee training in identifying these risks is critical. Employers should remind employees to never click on links or attachments if they do not know the sender, and to be careful of spoofing and hacking schemes. This website from the FBI provides good guidance: https://www.ic3.gov/preventiontips.aspx#item-13 ,

SPECIAL DATA SECURITY ISSUES

Almost two dozen states in the U.S. have statutes that require companies to engage in efforts to safeguard personally identifiable information. A number of U.S. federal laws, regulations and industry standards, including HIPAA, Gramm Leach Bliley (and the implementing Interagency Guidelines), and the Payment Card Industry Data Security Standards (PCI-DSS) require covered entities to engage in reasonable security efforts as well. In addition, some U.S. businesses may be subject to foreign laws containing data security requirements, including the European Union General Data Protection Regulation (GDPR). Further, the Federal Trade Commission has brought claims under the *unfairness* prong of Section 5(a) of the FTC Act based on failure to have adequate data security measures (*e.g.*, U.S. v. Choicepoint, Civ. Action No. 1 06-CV-0198 (ND Ga. 2006)).

Businesses must ensure that they adapt those security requirements to the new era of remote work, increased online services, and heightened cyberattacked and business email compromises. Not only are such measures important to comply with legislation and standards, such measures can help companies defend against negligence and other torts by impacted individuals and companies arising out of a data breach. For instance, where a vendor and its customer fall victim to business email compromise, resulting payments being wired to fraudulent accounts, recent cases have held that the party that was most responsible for, or who was in the

best position to avoid, the fraud will bear the loss. (*see, e.g. Beau Townsend Ford Lincoln, Inc. v. Don Hinds Ford, Inc.*, 759 Fed. Appx. 348 (6th Cir. 2018). Robust security measures and practices can help deflect responsibility for losses resulting business email compromise and other cyberattacks.

The NYDFS Cybersecurity Regulations contain some of the toughest and most detailed security requirements. The NYDFS recently published guidance on compliance in light of the pandemic. The guidance notes heightened risks in the areas of remote working and phishing and fraud. The guidance requires covered entities to make remote access as secure as possible under the circumstances, including the use of multi-factor authentication and secure VPN connections that will encrypt all data in transit. The guidance also requires that regulated entities ensure that devices used for telework are properly secured, including locking down the devices and installing appropriate security software, and that employees are reminded to not send Nonpublic Information to personal email accounts and devices. The guidance also notes the targeting of remote video and audio-conferencing applications by cybercriminals (think Zoom) and advises regulated entities to limit unauthorized access, and make sure that employees are given guidance on how to use them securely. To combat phishing, the guidance notes that regulated entities should update authentication protocols, particularly for high risk activities like security exceptions and wire transfers.

See https://www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness

See also PCI-DSS Guidance. https://blog.pcisecuritystandards.org/how-the-pci-dss-can-help-remote-workersutm_campaign=Blog&utm_source=hs_email&utm_medium=email&utm_content=85318447&_hsenc=p2ANqtz853oCnz1HiQpqoT3NZi_QSWblP4Xkg7X8FdexBAyraCXOU3TWlYLYo1nYdp24KIaIJRChR4RFYBzs-MeT5aglo0hKc64Q&_hsmi=85318447

VENDOR MANAGEMENT

In addition to tightening up their own privacy and data security practices, businesses need to consider the privacy and data security practices of their vendors. Under numerous laws and standards, including the EU Global Data Protection Regulation, the Gramm Leach Bliley Safeguards rule, and a handful of state data breach/security laws, businesses are responsible for imposing certain data security requirements on vendors in order to protect personally identifiable data and can be liable for the privacy failures of their vendors. This requires addressing new and emerging privacy and data security risks arising from COVID-19. The NYDFS guidance emphasizes this continuing oversight role: "The challenges created by the COVID-19 pandemic have also affected third-party vendors, and regulated entities should re-evaluate the risks to critical vendors. See 23 NYCRR § 500.11. Regulated entities should coordinate with critical vendors to determine how they are adequately addressing the new risks."

https://www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness .

Businesses should ensure that their contracts with vendors who will process, maintain or access personally identifiable data require the vendors to maintain appropriate safeguards to protect the data. Likewise, businesses need to consider any new risks presented by the pandemic. For example, before jumping on that next video conference, businesses should either determine that the conference vendor has adequate

measures in place to protect personally identifiable information or ensure that pii is not shared during the conference.

CONSUMER PRIVACY

Remote Advertising. With widespread government "stay at home" orders, remote advertising through email, texts and online tracking may be attractive to businesses. Companies, however, should keep in mind limitations on such advertising through laws such as CAN-SPAM, the Telephone Consumer Protection Act, and state consumer privacy legislation such as the California Consumer Privacy Act. In particular, the TCPA imposes certain restrictions on automated telephone calls and text messages to consumers, including requiring consumer's affirmative consent, as well as detailed disclosures if telemarketing. Given the reach of some marketing campaigns, TCPA violations can quickly spawn into consumer class actions for the unwary. Additionally, evolving consumer advertising privacy laws, such as Nevada's amendment to N.R.S. 603A.340 , continue to impose heightened obligations on businesses dealing with consumers. Nevada's amendment prohibits certain businesses operating websites that collect information from consumers in Nevada from selling covered information if so directed by the consumer.

Note also that online credentials and passwords can be protected personally identifiable information under U.S. state data breach laws. Companies that own, license or maintain online credentials in such states will have obligations to notify consumers if their online credentials are accessed by an unauthorized person. Several states recently revised their data breach notification laws to include online login credentials. *See e.g.* Oregon Consumer Information Protection Act (OCIPA) SB 684 (expands the definition of personal information to include "user names or other means of identifying a consumer for the purpose of permitting access to the consumer's account"); amendment to Washington's data breach notification law (HB1071) (personal information is expanded to include online login credentials); and New York Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) S5575B (personally identifiable information defined as a "username or email address in combination with a password or security question and answer that would permit access to an online account); *see also,* California Consumer Privacy Act, Cal Civ. Code 1798.140(o)(1)(A)("'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. .. including.. online identifiers")

Evaluating Customers for Signs of COVID-19 Infection. As government stay at home orders relax and businesses resume operations, retailers, office buildings, restaurants and entertainment establishments will look for ways to ensure that visitors are not putting employees and other guests at risk. Title III of the Americans with Disabilities Act (which prohibits discrimination based on disability by public accommodations), has an exception for persons who pose a direct threat to the health or safety of others. A direct threat is defined as a "significant risk" to the health or safety of others that cannot be eliminated by the modification of policies, procedures or practices or auxiliary aids. Businesses that are public accommodations will need to assess the significance of the threat by objective current medical evidence. Businesses should carefully consider Title III, and similar state laws, in making decisions on how to screen patrons and customers. Where questionnaires and temperature checks are permitted by applicable law, businesses should avoid linking the information to the patron's name or other identification and should properly dispose of the results.

Businesses also should keep in mind that health information can be protected personal information under the laws of some states. For example, the CCPA includes "health data…that includes identifying information" and an "individual's physiological, biological, or behavioral characteristics, …that can be used, singly or in combination with each other or with other identifying data, to establish individual identity" in its definition of biometric information. Cal Civ. Code 1798.140(b). Companies collecting such information therefore must comply with the applicable notice, consent and security requirements related to such data.

MISCELLANEOUS ISSUES

Extended Deadlines. Numerous government regulators are extending filing deadlines. The New York Department of Financial Services ("NYDFS") has extended from April 15, 2020 to June 1, 2020 the deadline for certifying compliance with the NYDFS' Cybersecurity Regulations for calendar year 2019. In addition, any NYDFS regulated entity or licensed person who previously filed a notice of exemption from compliance with the regulations does not need to refile the notice. Changes in status, however, should be reflected in an updated filing. https://www.dfs.ny.gov/industry_guidance/cybersecurity

Notably, the California Attorney General is *not* extending the July 1, 2020 enforcement deadline under the California Consumer Privacy Act ("CCPA"). Companies subject to the CCPA (http://www.mvadatapoints.com/the-wait-is-over-proposed-regulations-implementing-the-ccpa-are-released/) , must continue to implement the requirements of the CCPA.

Moore & Van Allen Privacy & Data Security team Karin McGinnis, karinmcginnis@mvalaw.com, (704) 331-1078
Todd Taylor, toddtaylor@mvala.com, (704) 331-1112
Neil Bloomfield, neilbloomfield@mvalaw.com, (704) 331-1084
Carol Ewald Bowen, carolbowen@mvalaw.com, (704) 331-2462
Bill Butler, billbutler@mvalaw.com, (704) 331-2455
Michael Coyne, michealcoyne@mvalaw.com, (704) 331-2494
Suzanne Gainey, suzannegainey@mvalaw.com, (704) 331-3559
Brandon Gaskins, brandongaskins@mvalaw.com, (843) 579-7038
Charles Jordan, charlesjordan@mvalaw.com, (843) 579-7030
Kimberly Kirk, kimberlykirk@mvalaw.com, (704) 331-3524
Marcus Lee, marcuslee@mvalaw.com, (704) 331-1066
Tandy Mathis, tandymathis@mvalaw.com, (704) 331-2329
Sarah Negus, sarahnegus@mvalaw.com, (704) 331-3667
Edward O'Keefe, edwardokeefe@mvalaw.com, (704) 331-1033
Leslie Pedernales, lesliepedernales@mvalaw.com, (704) 331-2461
Rome Perlman, romeperlman@mvalaw.com, (704) 331-3693
Sam Skains-Menchaca, samskains@mvalaw.com, (704) 331-3587
Henry Ward, henryward@mvalaw.com, (704) 331-1027
John Zaloom, johnzaloom@mvalaw.com, (919) 286-8182