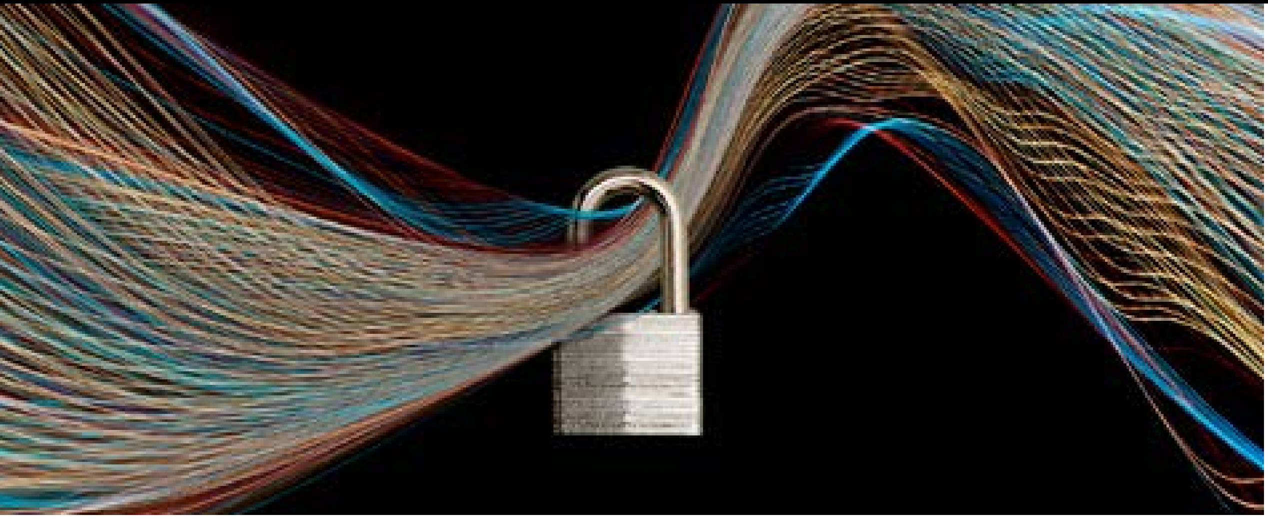

Returning to the Work Site: Cybersecurity and Privacy Considerations During the COVID-19 Pandemic

As businesses prepare to return to the work site after an extended period of closure and/or remote working due to the COVID-19 pandemic, they need to consider cybersecurity and privacy protection. There are a multitude of privacy and regulatory factors, data protection measures and insurance implications that should be part of any organization's return to work strategy.

Privacy and confidentiality regulations

Regulatory and enforcement bodies are attempting to balance public health and privacy rights when providing guidance to employers and consumers. Areas of consideration related to consumer and employee privacy include:

- Whether and when to conduct temperature scans.
- How to maintain records related to COVID-19 testing.
- Communication protocols regarding infected employees and/or consumers.
- Use of contact tracing applications.
- Compliance with various legal requirements and best practices.

The U.S. Centers for Disease Control and Prevention (CDC) and the Equal Employment Opportunity Commission (EEOC) have provided some interim guidance. Some of the CDC's interim guidance centers around coordination with state and local health officials in obtaining accurate information to formulate the appropriate response. Additionally, the CDC encourages employers to implement and update plans which: (1) are specific to your workplace; (2) identify all areas and job tasks with potential exposures to COVID-19; and (3) include control measures to eliminate to reduce such exposures.

The CDC has offered three privacy and confidentiality considerations to prevent stigma and discrimination in the workplace: (1) make employee health screenings as private as possible; (2) do not make determinations of risk based on race or country of origin; and (3) maintain confidentiality of each individual's medical status and history.

Testing/temperature scans

According to the EEOC, COVID-19-related testing of employees is a permissible medical examination. As such, appropriate handling of that information is required, including compliance with the Americans with Disabilities Act (ADA). More specifically, the EEOC advises:

- Employee temperature checks are allowed. However, employers should note that some people with COVID-19 do not present with a fever.
- An employer may choose to administer a COVID-19 test to employees before they enter the workplace. Employers should ensure the accuracy and reliability of the test.

As your organization considers testing and temperature scans, it is critical to understand the specific information you will be capturing. For example, if you capture more than a temperature, such as characteristics used for facial recognition, the implications and requirements to protect that type of biometric information may be different than those for other information being collected.

Health information protection

The EEOC considers information related to employee COVID-19 testing to be medical information. The EEOC takes the position that all employee medical information should be maintained in accordance with the ADA requirements. Specifically, the EEOC advises:

- The ADA requires all medical information regarding an employee to be stored separately from the employee's personnel file, in order to limit access to this confidential information. An employer may store all medical information related to COVID-19 in existing medical files, including an employee's statement that they have the disease or suspects they have the disease, as well as the employer's notes or other documentation from questioning an employee about symptoms.
- If an employer requires all employees to have a daily temperature check before entering the workplace, the employer may maintain the log of the results but must maintain the confidentiality of this information.

Communications regarding infected employees

The balance between confidentiality and public health again comes into play when employers must decide how and what to communicate regarding an infected an employee. The CDC advises, “[i]f an employee is confirmed to have COVID-19 infection, employers should inform fellow employees of their possible exposure to COVID-19 in the workplace but maintain confidentiality as required by the … ADA.” Some states have provided exemplars as to how to communicate in the event an employee has COVID-19. For example, California’s Department of Fair Employment & Housing issued the following exemplar:

> [Employer] has learned that an employee at [office location] tested positive for the COVID-19 virus. The employee received positive test results of this test on [date]. This email is to notify you that you have potentially been exposed to COVID-19 and you should contact your local public health department for guidance and any possible actions to take based on individual circumstances.

The EEOC has provided the following additional guidance on communications regarding infected employees:

- If an employer learns an employee has COVID-19, the employer may disclose the name of the employee to a public health agency.
- A temporary staffing agency or a contractor that placed an employee in a workplace may notify the business and disclose the name of the employee to the business as the business may need to determine if the employee had contact with others in the workplace.

Compliance

While businesses and consumers should pay particular attention to guidance from the CDC and EEOC, international, federal, state, and local laws and guidance must also be complied with, to the extent applicable. For example, some organizations will be required to comply with the Health Insurance Portability and Accountability Act and will need to look to the relevant guidance from the U.S. Department of Health & Human Services. Other organizations may have compliance obligations under the Family Education Rights and Privacy Act and will need to look to direction from the U.S. Department of Education. Moreover, many businesses will have compliance obligations as required by the Occupational Safety & Health Administration (OSHA) which has issued several directives regarding occupational illness during the pandemic, including recordkeeping requirements related to COVID-19 cases.

Organizations will also need to coordinate their approach with state and local government directives and guidance, and some will also have to look to the various international data protection authorities to help guide their return to work strategies on privacy and confidentiality.

Information and data security considerations

As organizations return to the work site, they should review, and possibly update, their information governance practices and data security protocols and procedures. Some protocols and practices to consider, include:

Standard security procedures

- Limit employee use of personal computers and devices (tablets, mobile phones, etc.) on company networks.
  - If personal computers must be used:
    - Install Network Access Control protocols to ensure that personal equipment does not introduce new cyber risks to the organization.
    - Ensure adequate endpoint detection and response protocols are in place.
    - Ensure all available software patches have been applied.
- Create a safe way for employees to copy relevant files from personal devices.
- Implement and enforce USB device control to prohibit use of USB storage devices on company networks.
- Instruct employees to securely delete any company or customer information that may remain on personal computing equipment.
- Inventory software on personal or company computers that may have been installed while employees were working from home to determine the risks it may present.
- Require passwords to be changed when employees return to the workplace.
- Review all individuals who have access to critical applications.
  - Confirm all users still require access to those critical applications.
- Identify all remote access accounts to all systems and applications.
  - Confirm all remote accounts still require access to systems and applications.
  - Request an updated list of contractors from your vendors that are still employed.
  - If any of your previous contractors are no longer with the vendor, revoke their access immediately.
  - Revoke access for all remote accounts that are no longer needed.

Training/education protocols

- After an extended period of working at home, employees should be refreshed on the company's cyber security policies and procedures.
- All employees need to be alert to phishing emails that concern return to work matters.
- Refresh and test your incident response program to include:
  - Incident reporting protocols (how and to whom your workforce reports incidents).

  - Incorporate your breach coach contact information within your incident response program.
  - Disseminate incident response roles and responsibilities to leadership and key stakeholders.
- Identify the stakeholder ultimately responsible for decision making in connection with the incident response and regarding whether your organization has sustained a data breach.

Insurance implications

Actions taken, or not taken, as employees return to work may have a cost. They may also result in claims by regulators, employees, and/or third parties. Broadly speaking, cyber policies will likely cover privacy-related claims. The policies will also cover expenses an organization incurs as a result of a cyber event, such as a data breach. Cyber policies will not cover the cost of implementing best practices and safeguards. However, cyber insurers often provide a variety of services that can help companies understand and mitigate their cyber risks. Now may be an excellent time for your organization to utilize such offerings.

Lockton's COVID-19 resources may be found at https://www.lockton.com/coronavirus.

While this paper discusses legal and regulatory issues and developments, it is not, and is not intended to be, legal advice. As an insurance broker, Lockton cannot and does not provide legal advice to clients and others. Advice concerning legal or regulatory matters must be obtained from legal counsel.

---

[1] https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html

[2] https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html

[3] https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html

[4] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

[5] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

[6] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

[7] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

[8] https://www.cdc.gov/coronavirus/2019-ncov/community/general-business-faq.html

[9] https://www.dfeh.ca.gov/wp-content/uploads/sites/32/2020/03/DFEH-Employment-Information-on-COVID-19-FAQ_ENG.pdf

[10] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

[11] https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws

[12] https://www.osha.gov/memos/2020-05-19/revised-enforcement-guidance-recording-cases-coronavirus-disease-2019-covid-19