

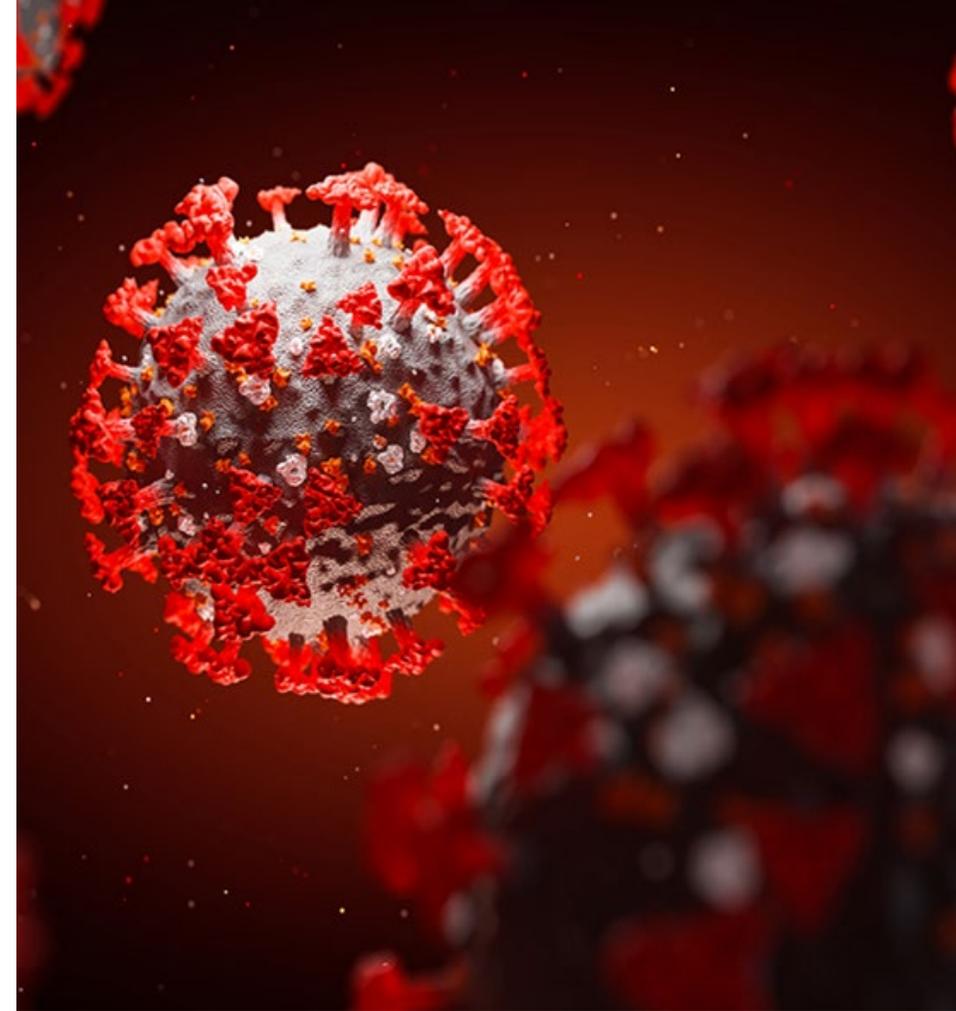
Mitigating Risk in Uncertain Times

- Remote Work Challenges
- Return to Work Challenges
- The Future of Disaster Recovery/Business Continuity



COVID -19-Key Points to Ponder

- Have you reviewed your insurance policy for coverages?
- Have you reviewed and tested your Business Continuity Management plans? If so, how did they fare?
- Have you considered the implications to your supply chain, and have you identified other suppliers?
- Have you activated your plans? If not, what would cause an activation?



COVID-19 Impact on Workplaces

Experience of Essential Employers

- Experiencing spread of the virus at work.

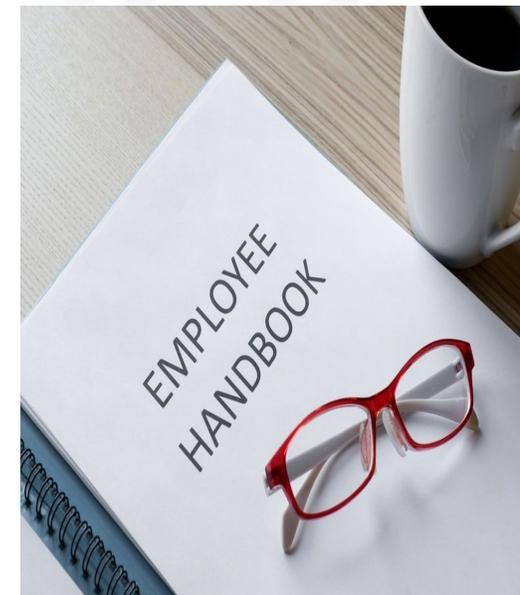
(Hot Spots in Certain Industries)

- High absenteeism due to quarantine/exposure.
- Employees experiencing anxiety over possible infection.
- OSHA complaints at record level.
- PPE difficult to source.
- **Employers simply didn't/don't know what to do.**



Employment Considerations/COVID-19

- Federal and State EEO laws not suspended in COVID-19 era.
- Heightened concerns re ADA (disability discrimination).
- Heightened risks of age and national origin discrimination.
- ADA medical confidentiality rules still apply.
- Employer rights for medical exams are broader in a pandemic.
- Employees with chronic health conditions entitled to accommodations due to heightened risk.
- Leave beyond Families First Coronavirus Response Act (FFCRA) may be a reasonable accommodation.



COVID=Legal Liability?

- Since March 12, there have been 638 lawsuits* (including 72 class actions) filed against employers due to alleged labor and employment violations related to the coronavirus.
- The filings have increased rapidly over the past several months.
- OSHA Whistleblower complaints up by 30%.

****Source: Littler Mendelson P.C***



What Can You Do?

- Follow U.S. (CDC) guidelines for businesses, including best practices for social distancing, cleaning and disinfecting the workplace, and quarantining.
- Note that specific guidelines apply to critical infrastructure workers.
- Use (OSHA's) most recent guidelines as a resource when creating return- to-work policies.
- Make sure employees know what measures the business is taking to protect them.
- Stay aware of employees' health while respecting their legal right to privacy.



What Can You Do?

- Keep reminding employees of the symptoms of COVID-19 and urge them to seek medical attention if they experience symptoms.
- Err on the side of transparency by informing employees of confirmed COVID-19 cases in the workplace while maintaining employees' privacy.
- Stay on top of current and evolving guidelines from the CDC, OSHA, the U.S. DOL and state and local governments.



Practical Approach to COVID in the Workplace

Most COVID-19 precautions are advisory in nature

- Objective should be to manage the risks associated with COVID-19.
- Plans should adapt to changing circumstances
- Practical approaches consider the circumstances

***Liability Protections dependent upon following guidance.**



Workplace Safety: OSHA Compliance

- Critical for “essential” and re-opening businesses. OSHA advises evaluating risks, using preventative measures
- OSHA’s Guidance for COVID-19 outlines:
 - ✓ Workplace and administrative controls
 - ✓ Recommended policies and practices
 - ✓ Required postings
 - ✓ Need for coordination and planning: internal and external communications



Could I? Should I?

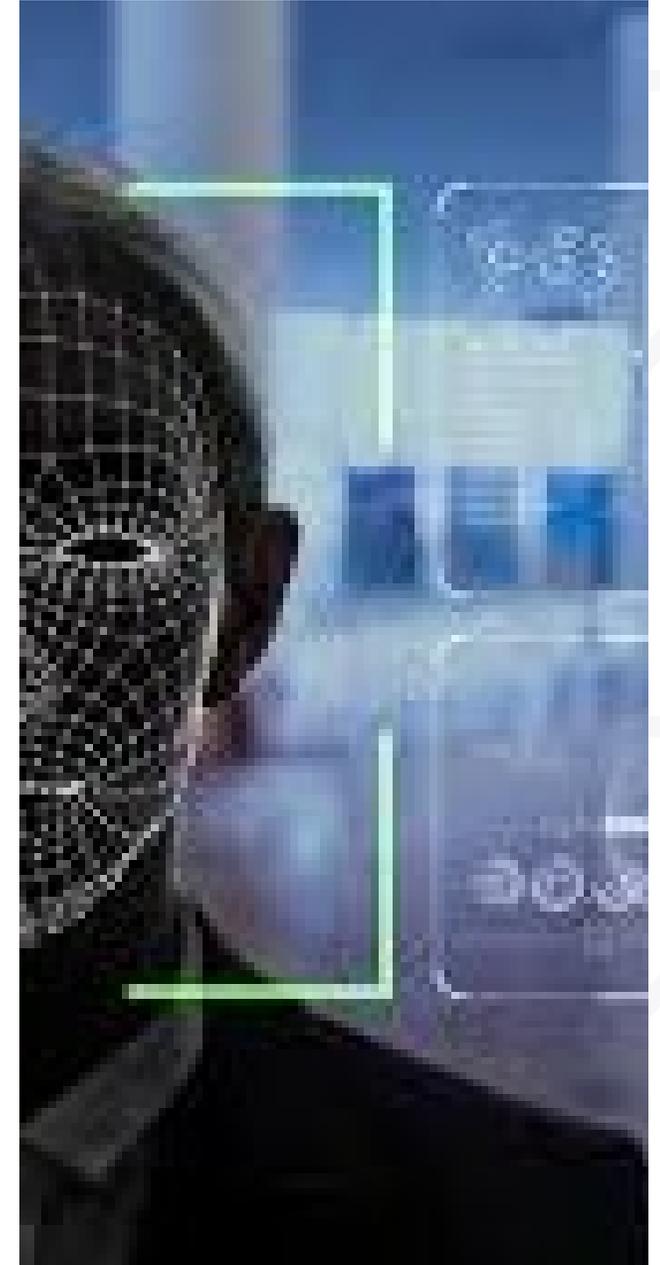
Screening Employees

- **Temperature Checks (Some States/Cities Require)**
 - ✓ Temperature Checks are imperfect, should be part of **overall** plan.
 - ✓ Must ask: who will do it, where, and what is the process for a “positive” reading?
 - ✓ Ensure worker safety of those performing checks, and the employees.
- **Self-Screening**
 - ✓ Questionnaire
 - ✓ More private-but relies on employee’s transparency.
- **What about contractors/visitors?**
 - ✓ Create communication policies about exposures, or potential exposures.
 - ✓ Be careful not to require too much information, but permissible to be informed of exposure/infection and mitigation efforts.



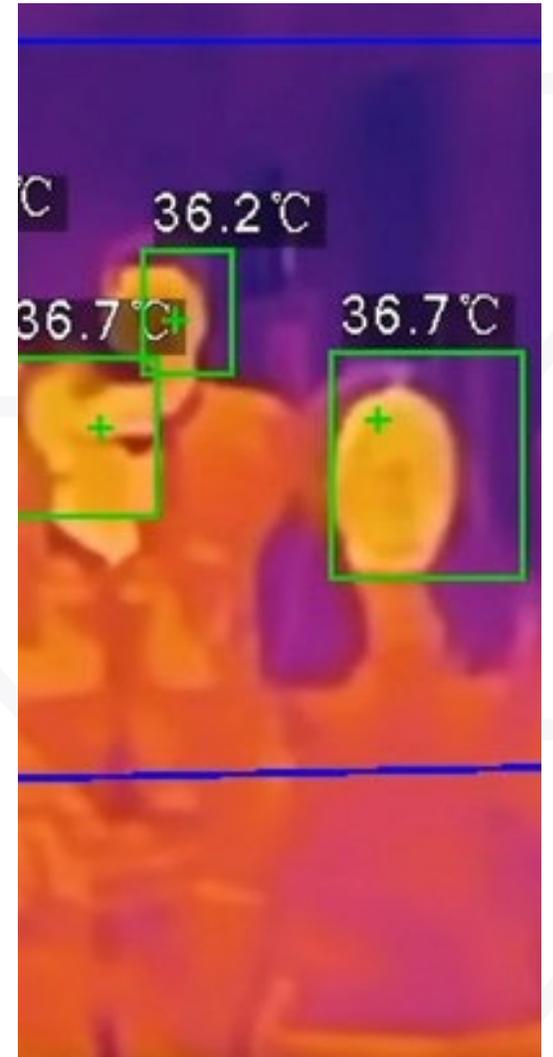
Privacy Issues- Now and Future

- Enormous amounts of data will likely be collected as part of reopening procedures.
- Data likely to be collected include:
 - ✓ Temperatures of visitors/guests/customers
 - ✓ Observations regarding behavior/actions of the same
 - ✓ Similar biometric data to measure enforcement and effectiveness of social distancing measures
 - ✓ Collection of identification data may be needed as well for “contact tracing” purposes



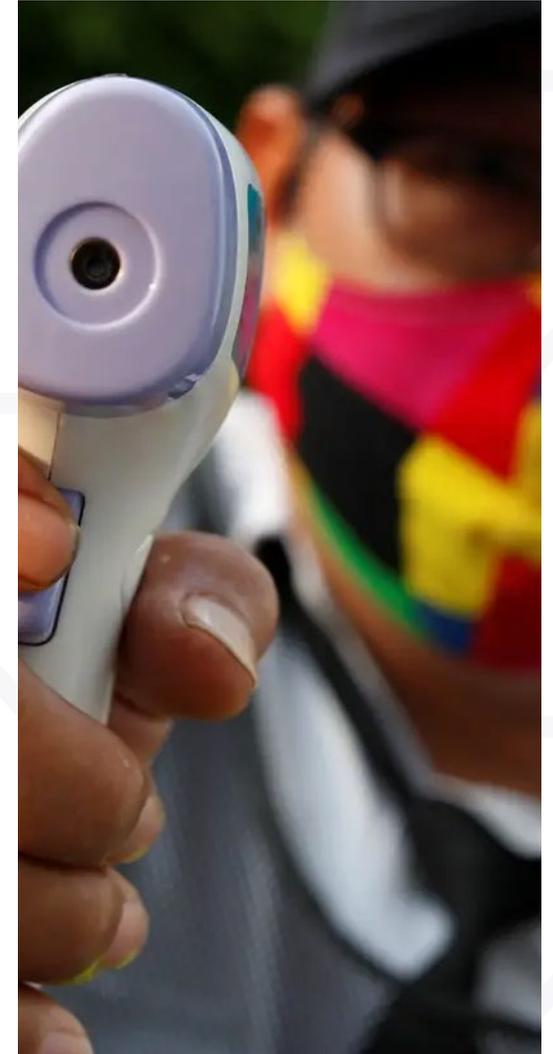
Potential Pitfalls of Data Collection

- Increasing number of states expanding the definition of “personal” information:
- California Consumer Privacy Act (CCPA)
- NY SHIELD law
- In some states, “personal information” much broader than before:
 - ✓ Includes biometric data, which is being defined very broadly
 - ✓ Failure to obtain consent (where required), protect, or even delete information could lead to claims of privacy violations.



Privacy Protection Considerations

- First and foremost, do not store or retain data unless absolutely necessary.
- If you do collect data, make sure to follow applicable state regulations on:
 - Consent (If mandated)
 - Protection of data
 - Required disclosures
 - Obligations regarding sharing or deletion of data



Responding to Safety Concerns

- Ensure that employees have multiple avenues to immediately raise health and safety concerns.
- Employees should never be disciplined or terminated because they voiced complaints about workplace conditions or practices, including concerns regarding COVID-19.
- There may be independent, non-retaliatory reasons for taking adverse action against an employee who also previously raised health and safety concerns, but any decision regarding the adverse action should not or be influenced by the health or safety complaint.
- If independent reasons justify disciplinary action against an employee who recently raised concerns, the employer should ensure the reasons are properly documented, consistent with the company's policies and procedures, and that other employees who have engaged in similar conduct—but who have not complained of health and safety concerns—received the same disciplinary action. TAKE A STEP BACK....Evaluate....Then move forward...



Responding to Safety Concerns

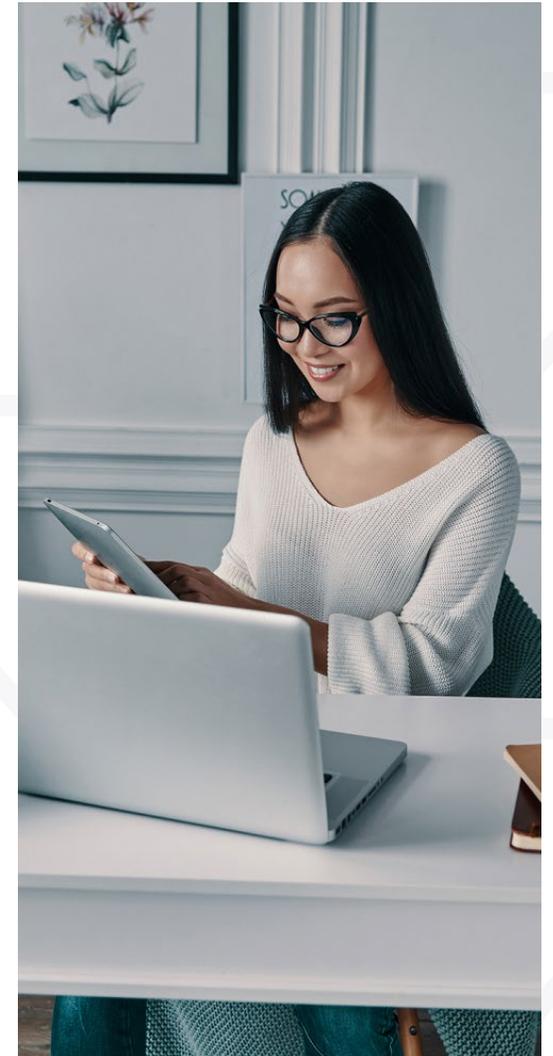
- In turn, be certain that the specifics of health and safety complaints are appropriately documented – including the time and date, the recipient of the complaint, and the specifics of the concerns that have been raised.
- Confirm and update the company's procedures for referring or escalating health and safety complaints to the appropriate department or individual, and for investigating and addressing concerns that have been raised.
- Take health and safety complaints seriously. Remind front-line supervisors to objectively listen to concerns that have been raised, and to appropriately refer and escalate the concerns consistent with the company's procedures to HR.



Remote Working: The New Normal*

- 55% of businesses globally offer some capacity for remote work
- 77% of telecommuters report being more productive
- 30% of telecommuters save upward of \$5,000 a year
- \$11,000 - companies can save annually for each employee that works remotely at least half-time.
- 99% of remote workers want to continue telecommuting in the future
- 90% of remote workers would recommend working remotely to a friend
- In the U.S remote work has risen by 173% between 2005 and 2018

**Research done by Gartner, Flexjobs, Owl Labs*



Remote Work Challenges

Have the employee designate a particular area in the home as the "home office."

- Have the employee complete regular time sheets as a record of the hours worked (if non-exempt).
- Have the employee be mindful of ergonomic issues in the home work area.
- Implement formal agreements-stating the hours that will be worked and the expectations.



2 Extremes of Remote Workers

1. Employees who use most of their day to attend to personal matters and don't get much work done.

OR....

2. Employees who don't know when to "turn it off" and end up working more than 40 hours because the office is right there and create obligations to pay overtime...



Additional Future Challenges?

- Conversations that may have taken place around a water cooler may now be reduced to writing, whether via text message, email or even messages exchanged within a video conferencing platform. *(A quick email reminder to remote workers, reminding them to treat communication during remote work as they would any other workplace communication is a good idea.)*
- ***Workmen's Comp?? ...Workplace Violence??***



Cybersecurity 101- Remote Workers

- When creating new accounts for home workers, ensure strong passwords are set and use the *principle of least privilege* to reduce risk.
- Enable two-factor authentication.
- Ensure workers can connect through VPNs and there are sufficient licenses and bandwidth.
- Make sure VPN software is patched and the latest version is installed. Ensure procedures are in place to keep the software updated.



Cybersecurity 101- Remote Workers

- Consider disabling USB ports to prevent the use of portable storage devices. This will reduce the risk of malware infections and the risk of data theft.
- Ensure portable devices are protected with encryption. Use software solutions that lock devices in the event of theft or allow devices to be remotely wiped.
- Ensure you set up communications channels to allow remote workers to collaborate, such as teleconferencing, chat facilities, document sharing platforms, and SaaS applications. Make sure employees are aware of what can and cannot be shared via chat apps such as Slack and Google Chat.

“HOME NETWORKS ARE SOME OF THE MOST HOSTILE NETWORKS ON THE PLANET....”



Cybersecurity 101- Remote Workers

- Ensure staff are trained on new applications, the use of VPNs, and are aware of the additional risks from remote working.
- Train remote workers on how to identify phishing and other cybersecurity threats. (***Social Engineering may be the biggest threat ...***).
- Ensure policies and procedures are set up for reporting threats to IT security teams. Instruct employees on the correct course of action if they believe they have fallen for a scam.
- Implement a DNS filter to prevent employees from accessing high risk websites on corporate-issued devices and block downloads of risky file types.



Returning to Work Challenges

- As infections decline, some employers will transition back to the traditional workplace.
- Employers are concerned about the issues involved in returning to the workplace.
- Lessons learned by essential employers will help these employers avoid mistakes.



Exposure Control Plan - Elements

Your **WRITTEN** plan should include:

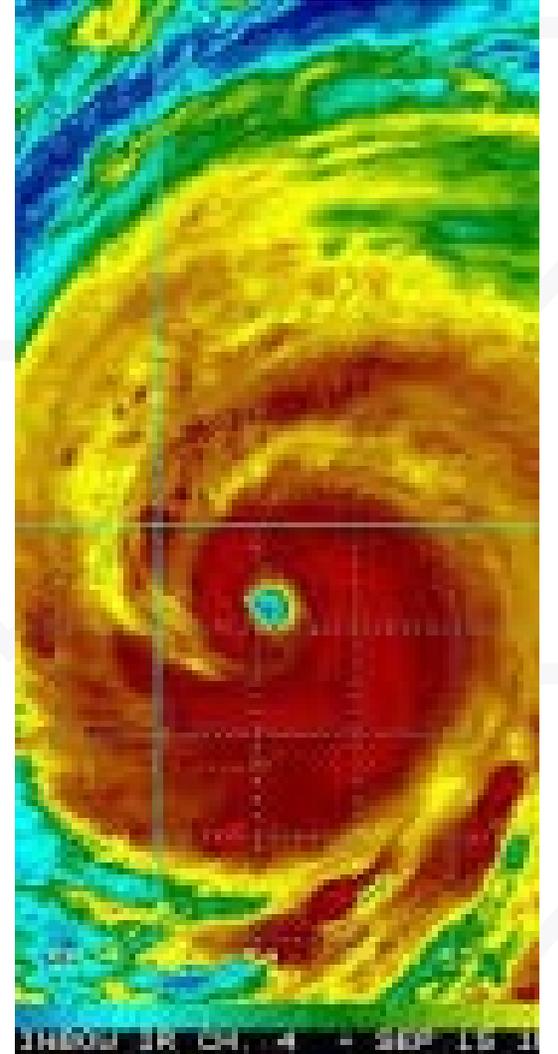
- Infection prevention
- Identification/isolation of infected persons
- Engineering, administrative controls, PPE
- Cleaning and disinfection
- Communication and training
- Periodic audits (is it working??)



Recovery Plans- Traditional v. Pandemics

Traditional Planning:

- Incident focused – fire, flood, system outage etc.
- Relocating critical staff to offsite-location.
- Assumes defined physical area of impact.
- Assumes supply chain available.
- Most assume restoration of business within a short timeframe; not more than 30 days.



Pandemic Business Continuity Planning:

- **People focused** – How to stay operational if critical staff / significant numbers of staff are unavailable?
- Critical employees may be too ill to communicate.
- Assumes global impact.
- Employee care requirements – isolate, decontaminate and communicate.
- Supply chain deeply impacted.
- Recovery timeframes and length of quarantine, travel bans, etc. are unknown.



Pandemic Business Continuity Planning:

- Identify key roles that require on-site access, plan a backup in case of their absence.
- Design measures to help employees with management of stress and stressful situations.
- Arrange a method of assigning and distributing employees at various levels of operational reduction.
- Set up access for employee mobility (division of shifts, transport, etc.)



One final question to ponder.....

- How resilient are your partners and vendors?
- “Force Majeure”/Pandemic Clauses in current agreements?
- Will they survive the next pandemic/global crisis?



For further information please visit
www.dsisecurity.com/contact

