

## U.S. Return to Work Checklist

This checklist has been prepared to aid companies in creating a reasonable plan for balancing workplace safety obligations, anti-discrimination obligations, employee accommodation and leave obligations, data protection and privacy obligations, and record retention obligations as they bring employees back to work as State “Stay at Home” Orders related to COVID-19 are lifted.

### Workplace Safety

- Conduct COVID-19 Hazard Assessment
  - Analyze applicable state temperature screening, health screening, and face mask obligations and recommendations
  - Consider OSHA and CDC COVID-19 guidance
  - Identify potential workplace hazards related to COVID-19
  - Determine whether engineering controls, administrative controls, safe work practices and personal protective equipment are needed
  - Develop and implement procedures for managing employees in the workplace who are either suspected or confirmed to have COVID-19, including procedures related to:
    - Closing off areas used for prolonged periods of time by the sick employee for 24 hours
    - Cleaning and disinfecting the workplace
    - Informing other employees who may have been exposed
    - Determining when exposed employee(s) may return to the workplace
- Implement Appropriate Controls
  - Select and implement engineering controls, administrative controls, and safe work practices, and provide personal protective equipment, if necessary
  - Develop procedures for managing employees in the workplace who are either suspected or confirmed to have COVID-19, including procedures related to:
    - Closing off areas used for prolonged periods of time by the sick employee for 24 hours
    - Cleaning and disinfecting the workplace
    - Informing other employees who may have been exposed
    - Determining when sick and exposed employees may return to the workplace
    - Determining whether employee COVID-19 illnesses are work-related, and thus recordable on OSHA Form 300
- With respect to temperature and health screening process, limit data collected to that which is necessary to determine employees’ potential exposure to COVID-19

- If requiring employees to complete health screening questions prior to coming into the workplace, comply with applicable payment obligations under the Fair Labor Standards Act

### **Anti-Discrimination**

- Comply with ADA Anti-Discrimination Requirements
  - Continue to accommodate employees with known disabilities
  - For employees requesting a new accommodation, engage in an interactive process with employee to address all such employees' needs

### **Employee Leave**

- Comply with applicable Families First Coronavirus Response Act and Family and Medical Leave Act requirements
- Comply with obligations under applicable state paid sick and sick time laws and under Public Health Emergency Declarations

### **Notice**

- If collecting data from any California residents, at or before point of collection of COVID-19-related information from employees, provide CCPA-compliant Notice at Collection addressing the categories of personal information to be collected and the purposes for which the personal information will be used

### **Consent**

- If collecting employee medical information from a health care provider or health care service plan, obtain a signed CMIA-compliant authorization before doing so
- If utilizing a third-party vendor that is a covered entity under HIPAA to collect or process any COVID-19-related information, obtain a HIPAA-compliant authorization from each employee whose data will be collected or processed by such covered entity before collecting any such information

### **Confidential Data Storage**

- Maintain employee medical information as confidential medical records kept in separate files from other employee personnel files
- Store all medical information related to COVID-19 in such individual confidential medical files

### **Limited, Secure Data Sharing for Personnel with COVID-19**

- Take steps to help ensure that neither the identity of an employee who has tested positive for COVID-19, nor anything about his or her medical condition or symptoms, is disclosed to any customers and/or employees, with the exception of employees who require the information to perform their job duties and the employee's supervisor or manager, who may be informed in order to implement any necessary work restrictions or necessary accommodations
- Inform specific employees and/or customers that a person with whom they were in contact has tested positive for COVID-19 (without disclosing any identities)
- Limit personal information shared with government officials to information that is required to be shared

- Implement reasonable security measures to help ensure any employee personal information that is shared is shared in a secure manner

### **Data Security, Including Access Restrictions & Authentication Requirements**

- Implement and maintain reasonable security safeguards to protect employee medical information from unauthorized access, acquisition, destruction, use, modification, or disclosure

### **Third-Party Contracting & Management**

- If employee medical information is disclosed to any third-party vendor, confirm such vendor has an appropriate information security program in place to protect the confidentiality of such information
- Confirm the contract with any such third-party vendor requires the vendor to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information disclosed; and reasonably designed to help protect the information from unauthorized access, use, modification, disclosure, or destruction
- Implement a reasonable method of monitoring any such third-party vendors to help ensure the vendor's information security program operates in a manner reasonably calculated to prevent unauthorized access to or use of employee medical information

### **Records Retention**

- Take steps to help ensure employee medical information is retained in compliance with applicable retention periods

### **Secure Data Disposal**

- Take steps to help ensure all employee medical information, including information in the possession, custody, or control of any third-party vendor, is:
  - Completely and permanently disposed of within a reasonable amount of time after no longer needed for business purposes; and
  - Securely destroyed by shredding, erasing, or otherwise modifying the information to make it unreadable or indecipherable through any means

---

This checklist is intended to highlight key actions that should be considered in the context of returning employees to work, rather than to be an exhaustive list of all recommended U.S. Return to Work steps. This checklist is for general informational purposes only. The information provided does not, and is not intended to, constitute legal advice. This checklist may not contain the most up-to-date legal advice or other information. Readers should contact their attorneys to obtain advice with respect to their specific issues. No reader should act or refrain from acting on the steps in this checklist without first seeking legal advice from counsel. Only your individual attorney can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your unique situation. Use of, and access to, this checklist does not create an attorney-client relationship between the reader and Laura Clark Fey ([lfey@feyllc.com](mailto:lfey@feyllc.com)) or Fey LLC.

Copyright © 2020 Fey LLC. All rights reserved.