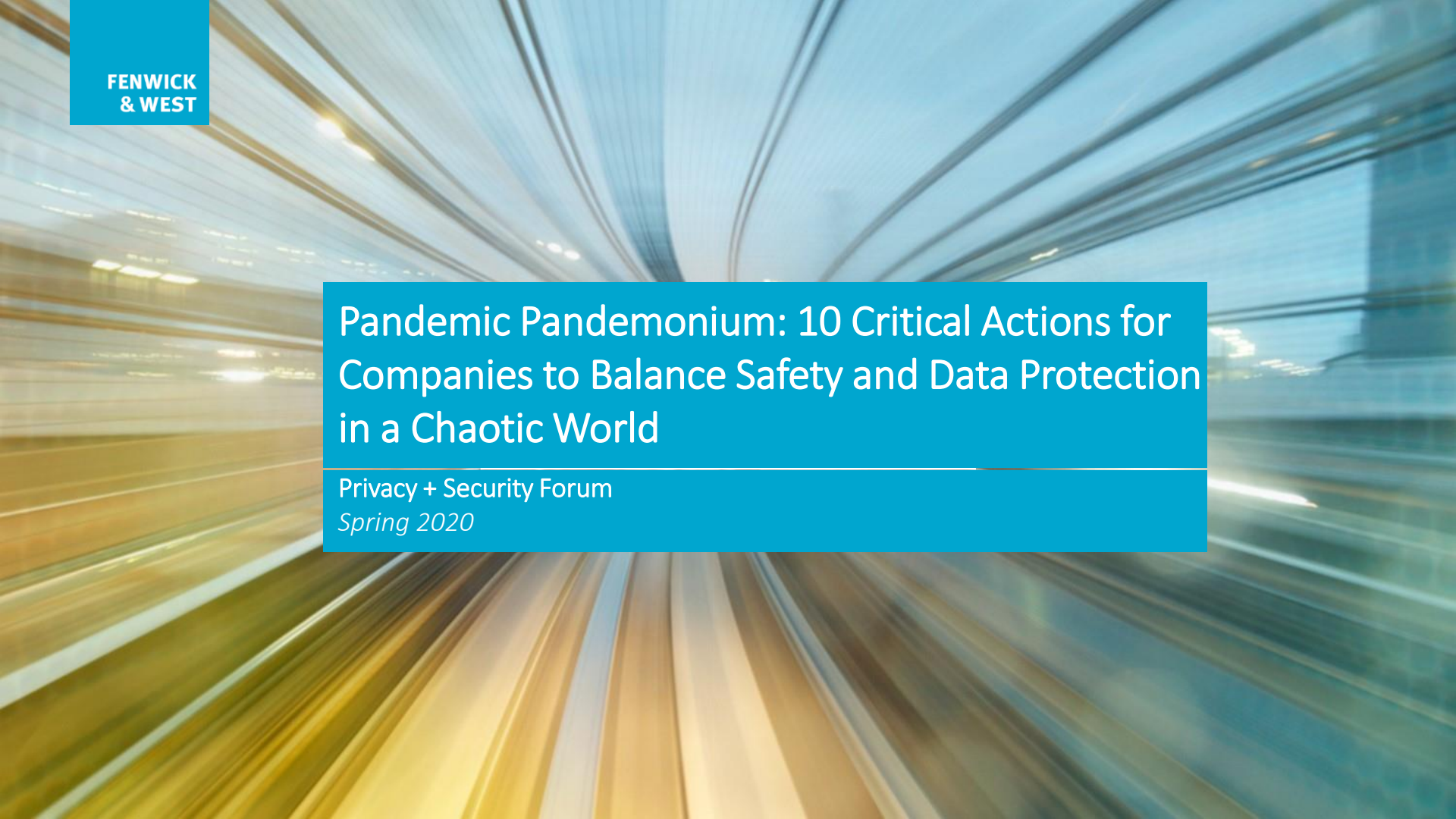


FENWICK & WEST

Pandemic Pandemonium: 10 Critical Actions for Companies to Balance Safety and Data Protection in a Chaotic World

Privacy + Security Forum

Spring 2020

Introductions - Moderators

Jim Koenig
Partner and Global Co-Chair
Privacy and Cybersecurity Practice
610.246.4426
jkoenig@fenwick.com

Jim Gregoire
Managing Director
Privacy and Cybersecurity Practice
424.225.1015
jgregoire@fenwick.com

Leading provider of assistance with global compliance, regulatory investigations, enforcements (e.g., assisting companies with OCR, FTC, FCC, SEC, Attorneys General, and others) and class actions.

Top in Technology – Named Technology Group of the Year by Law360 for the fifth consecutive year (2018)

- **One of the leading privacy & cybersecurity groups in the United States"** The Legal 500 (2018, 2019)
- **Jim Koenig and Jim Gregoire** recognized for Cyber Law (including Data Privacy and Data Protection) by *The Legal 500* (2019)
- **James Koenig "is exceedingly pragmatic** and has a time-tested methodology to scope a project, evaluate risk and resolve issues." Rated by Chambers & Partners Chambers 2020 (Global and US), 2019 (US)

Fenwick's Privacy & Cybersecurity Practice uniquely brings together industry CPOs/CISOs, regulatory and consulting experts and data architects to solve and implement today's emerging privacy and security challenges.

Introductions - Panelists

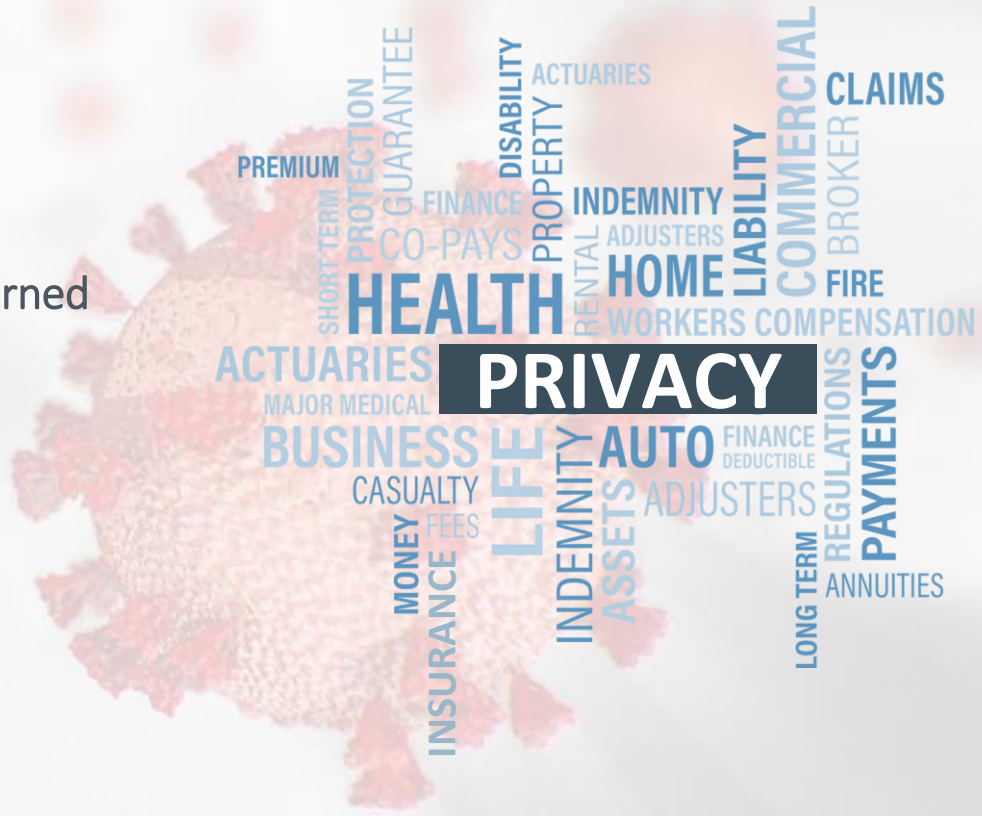
Amrita Srivastava
Associate General Counsel-US
Coupang

Charlie Britt
Senior Privacy Counsel
NCR Corporation

Zoe Strickland
VP Global Privacy &
US Commercial Compliance
Cigna

Henry Schober
Global Privacy Director and Data Protection Officer
Align Technology, Inc.

Table of Contents



Overview

Companies worldwide are working diligently to respond to the current global COVID-19 pandemic, addressing critical and monumental health and safety risks, coping with operational and logistical challenges presented by erratic and/or reduced customer activity, and supporting remote employee working.

Challenges

Procedures. Draft procedures quickly with clear guidelines.

Conflicting and Evolving Guidance. Juggle guidance from public officials, law enforcement, health organizations, and global regulatory agencies.

Emerging Trends. Monitor and understand rapidly evolving landscape.


FENWICK
& WEST
SUMMARY OF
REGULATORY GUIDANCE

Regulatory Guidance in 60+ Countries and Differing Approaches to Processing Activities

Regulatory agencies in different jurisdictions have issued guidance that varies in the level of restrictiveness for processing of health-related data for COVID-19. This table summarizes common elements or perspectives for each level of restrictiveness. (Note: Some slight variations across jurisdictions may exist. Not all jurisdictions are represented.)

More Restrictive (6)		Neutral (25)		Less Restrictive (23)	
Belgium	Luxembourg	Argentina			
Estonia	Netherlands	Australia	Iceland	Albania	
France	Peru	Austria	Jersey	Bermuda	Philippines
		Bulgaria	Malta	China	Poland
		Canada	Mexico	Denmark	Romania
		Cayman Islands	New Zealand	European Union	Russia
		Croatia	Norway	Hong Kong	Singapore
		Czech Republic	Portugal	Ireland	South Africa
		Finland	Slovakia	Israel	Spain
		Germany	Slovenia	Italy	Switzerland
		Gibraltar	Sweden	Japan	United Kingdom
		Greece	Turkey	Latvia	United States
		Hungary	Uruguay	Lithuania	UAE
• **No systematic or generalized data collection** (e.g., mandatory temperature readings and medical questionnaires) • **Identity of employees** affected must be kept confidential • Sensitive data of a patient can only be disclosed / revealed with **consent**.		• Personal information collected for COVID-19 prevention may be **used only for these purposes** and should be deleted after the end of the pandemic • Processing is permissible if necessary to protect the **vital interests** of the data subject or third parties (the general public) • Processing must be **proportional, adequate, relevant** and limited to minimum necessary • Disclosure of a patient name requires **consent unless permissible by data protection laws**			• Employers can collect and disclose **travel, symptom, interaction information** (and confirmed cases) in accordance with the anti-contagion safety protocols • Personal data can be collected, used and disclosed **without consent** to carry out contact tracing and other response measures • **Recorded images** can be processed and exchanged among data controllers and law enforcement institutions • In some jurisdictions, the processing of **location data** is permissible	

Data Collection & Prevention Efforts

Don'ts. Generally sensitive or restricted practices:

- ✘ Recording temperatures taken
- ✘ Conducting employee/worker health surveys asking questions relating to family members and others living in the home
- ✘ Requesting and collecting information about employee/worker social interaction and information about locations visited outside of work

Do's. Generally acceptable and/or recommended practices:

- ✓ Taking non-recorded temperature readings and recording only people with temperatures sent to home quarantine
- ✓ Conducting health surveys of employees and other workers, including asking them if they are experiencing symptoms of the virus, such as fever and shortness of breath
- ✓ Requiring home quarantine for people suspected of coming into contact with someone with COVID-19 and/or exhibiting symptoms (i.e., temperature, dry cough or other symptoms) or otherwise not feeling well
- ✓ Requiring a doctor's note to certify fitness-for-duty to return to work
- ✓ Using cell phone tracking software to track location information and confirm home quarantine compliance for people with COVID-19 (Israel only). Consent to collect precise location information may be required in some countries

Disclosures of Names of Individuals with Confirmed or Suspected Cases

Don'ts. Disclosure of impacted individuals should never be made to:

- ✘ Co-workers and other company personnel (disclosures to co-workers should not focus on the name of the individual impacted, but should rather focus on the location (i.e., office, building)) and the people who should closely monitor their health as they may have come in contact with one or more individuals who potentially had the virus
- ✘ Executives and direct supervisors, to the extent possible and on a need-to-know-basis under the circumstances

Do's. Disclosures of the name of the impacted individual should only be made in three limited circumstances:

- ✓ To health and safety government agencies without consent of the individual in cases of confirmed illness
- ✓ To healthcare providers with consent of the individual to aid the individual's treatment
- ✓ To family members with consent of the individual to help the family protect themselves and/or aid the individual's treatment

Remote Working / Work at Home

FTC and Global Guidance. The Federal Trade Commission and regulators in other countries have issued guidance regarding security practices for the home as most employees have started working there instead of the office. This is especially difficult in regulated industries that process credit card, health information, or other regulated data.

	Recommendations for Remote Working	United States	France	Luxembourg	Iceland	Ireland	Poland	Spain	Sri Lanka	Austria	Denmark
Employee	✓ **Complex Passwords & Up-to-Date Security.** Use complex passwords on devices and keep your security and operating system software up-to-date.	X			X	X			X		X
	✓ **Router Encryption.** Enable home router encryption to protect information sent over wireless network.	X	X						X	X	X
	✓ **Secure Physical Files.** Keep physical files locked and dispose of paper records securely (shred rather than using trash bin).	X			X	X				X	X
	✓ **Follow Employer Security Practices.** Follow the same security protocols that your employer has implemented at the office.	X			X	X					X
	✓ **Rely on Trusted Networks and Cloud Services.** Where possible only use your organization's trusted networks or cloud services, including through remote desktops.		X		X	X			X		X
Employer	✓ **Provide Training and Communication.** Employers should promote secure working from home methods through training and communication (including policies).		X	X			X	X			X
	✓ **Device Protection.** Ensure laptops and mobile devices are password-protected, locked, and secured and have appropriate access controls. When devices are lost or stolen, take steps to remotely wipe device memory.	X	X		X	X			X	X	X

Returning to the Workplace

Do's. Follow the approach outlined below, which is based on guidance from the Centers for Disease Control and Prevention (CDC), the Equal Employment Opportunity Commission (EEOC), and global data protection authorities, to comply with applicable regulations and best practices:

✓ **Testing**. Measure or verify employee/worker wellness through temperature readings.

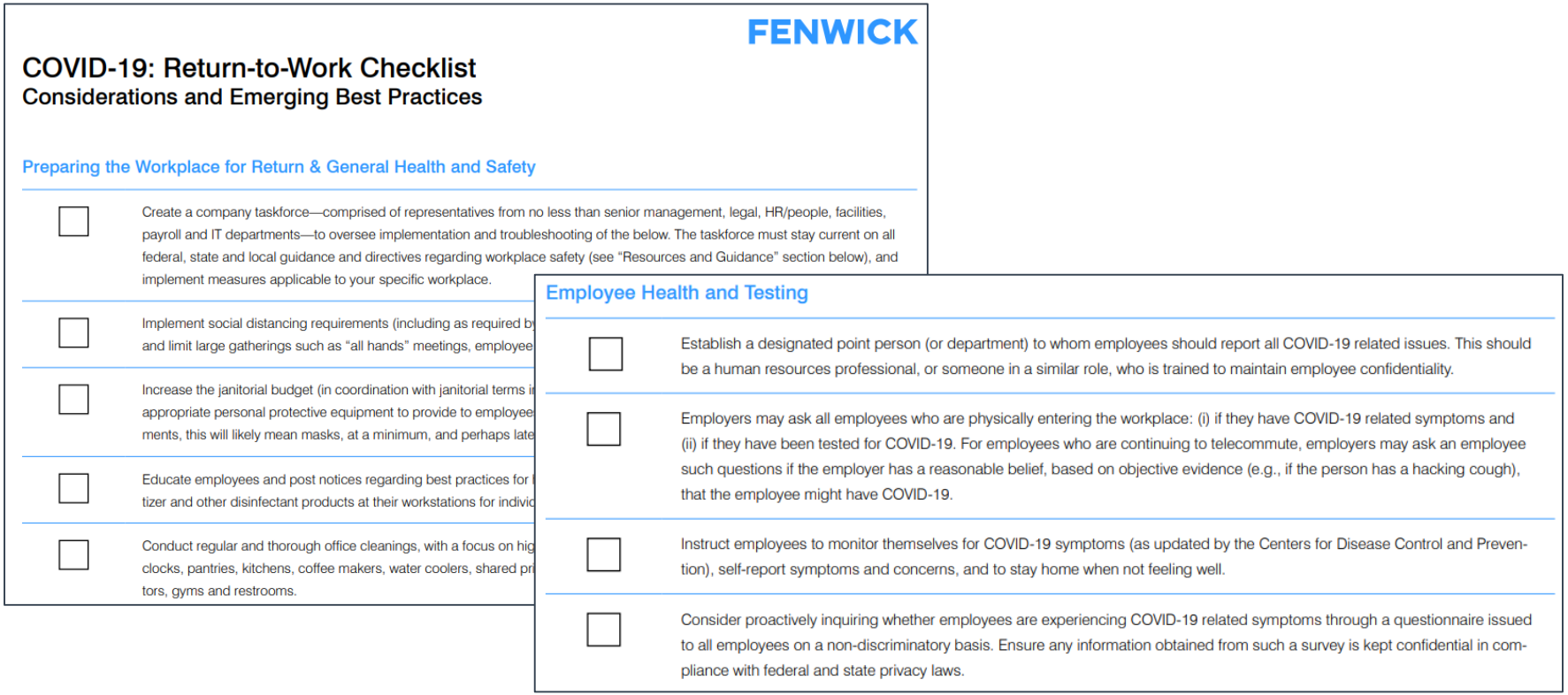
- Be transparent to employees (communicate protocol, provide privacy notice, set temperature threshold for consistency)
- Obtain consent to the performance of the testing
- Minimize invasiveness (e.g., through contactless thermometers)
- Appoint a designated tester – ideally an on-site medical staff person or other medical professional (e.g., R.N., M.A.) if possible
- Designate a testing site to preserve privacy and maintain distancing
- Limit recordkeeping to only suspected or confirmed cases; store records separately from personnel records and treat as a confidential medical record.

Returning to the Workplace (cont.)

Do's. Follow the approach outlined below to comply with applicable regulations and best practices:

- ✓ **Office Strategy**. Develop an office strategy for minimizing risk going forward. Options include:
  - Staggering employee returns
  - Maintaining social/physical distancing in the office (e.g., don't sit in cubicles next to each other)
  - Continue heightened cleaning, including all frequently touched surfaces
  - Require infection control practices (e.g., regular hand washing, PPE such as masks, discourage handshaking)
  - Provide necessary supplies to employees (e.g., tissues, no-touch disposal receptacles, soap and water, hand sanitizers).
  - Place posters that encourage good hygiene practices
- ✓ **Contact Tracing**. Track individual contact using technology.
  - Encourage (not require, unless by law) participation
  - Collect the minimum data needed to effectively trace
  - Enforce tight access controls to the data, limiting to a small group or health authorities only
- ✓ **Disaster Recovery Resumption**. Approach the return-to-work situation in the same way you might for disaster recovery
  - Define the "new normal" for the company
  - Identify adjustments made during the pandemic that may need to be discontinued (e.g., access controls, subscriptions/memberships)
  - Consider using a questionnaire for planning purposes
- ✓ **Remote Working**. Encourage continued remote working, especially for at-risk groups.

Return-to-Work



FENWICK

COVID-19: Return-to-Work Checklist
Considerations and Emerging Best Practices

Preparing the Workplace for Return & General Health and Safety

- ☐ Create a company taskforce—comprised of representatives from no less than senior management, legal, HR/people, facilities, payroll and IT departments—to oversee implementation and troubleshooting of the below. The taskforce must stay current on all federal, state and local guidance and directives regarding workplace safety (see "Resources and Guidance" section below), and implement measures applicable to your specific workplace.
- ☐ Implement social distancing requirements (including as required b
and limit large gatherings such as "all hands" meetings, employee
- ☐ Increase the janitorial budget (in coordination with janitorial terms i
appropriate personal protective equipment to provide to employee
ments, this will likely mean masks, at a minimum, and perhaps late
- ☐ Educate employees and post notices regarding best practices for
tizer and other disinfectant products at their workstations for indivi
- ☐ Conduct regular and thorough office cleanings, with a focus on hig
clocks, pantries, kitchens, coffee makers, water coolers, shared pr
tors, gyms and restrooms.

Employee Health and Testing

- ☐ Establish a designated point person (or department) to whom employees should report all COVID-19 related issues. This should be a human resources professional, or someone in a similar role, who is trained to maintain employee confidentiality.
- ☐ Employers may ask all employees who are physically entering the workplace: (i) if they have COVID-19 related symptoms and (ii) if they have been tested for COVID-19. For employees who are continuing to telecommute, employers may ask an employee such questions if the employer has a reasonable belief, based on objective evidence (e.g., if the person has a hacking cough), that the employee might have COVID-19.
- ☐ Instruct employees to monitor themselves for COVID-19 symptoms (as updated by the Centers for Disease Control and Prevention), self-report symptoms and concerns, and to stay home when not feeling well.
- ☐ Consider proactively inquiring whether employees are experiencing COVID-19 related symptoms through a questionnaire issued to all employees on a non-discriminatory basis. Ensure any information obtained from such a survey is kept confidential in compliance with federal and state privacy laws.


FENWICK
& WEST
COMPANY CHALLENGES &
LESSONS LEARNED

Mini-Roundtable Question 1:
Product Innovation and Operational Changes

What have been some of the most significant product, service and business changes you have made during the pandemic?

- Customer Interaction
- Variations for Different Geographies
- Warehousing / Supply Chain Management
- New Products and Creative Solutions
- Staffing
- Temporary vs. Permanent Changes

Mini-Roundtable Question 2:
COVID-19 Information Collection, Use, and Disclosure

Describe your company's approach to COVID-19 information collection, use, and disclosure?

- Testing (who, when, where, etc.)
- Questionnaires/Surveys
- Privacy Notices
- Tracking/Tracing
- Internal Points of Contact

Mini-Roundtable Question 3:
Remote Working / Work-at-Home

What measures has your company enacted to ensure security for data while employees are working remotely?

- Equipment
- Security
- Videoconferencing

Mini-Roundtable Question 4:
Return-to-Work

What is your company doing or contemplating for return-to-work?

- Office Strategy
- Staggered Returns
- Mandatory Testing
- Doctor's Note


FENWICK
& WEST
10 CRITICAL ACTIONS
TO TAKE NOW

10 Critical Actions to Take Now

1. Monitor Local, Regional, and National Conditions and Requirements

- Keep track of local, regional, and national conditions to remain compliant with applicable laws and to ensure responsiveness and adaptivity (e.g., in re-opening offices or stores)

2. Identify a testing frequency and location that allows employees to maintain social distance requirements and preserves privacy

- Always obtain consent to perform testing
- Minimize invasiveness (e.g., through contactless thermometers)
- Appoint a designated tester – ideally an on-site medical staff person or other medical professional (e.g., R.N., M.A.) if possible
- Specify thresholds for being sent home

10 Critical Actions to Take Now (cont.)

3. Communicate & Be Transparent with Employees and Customers

- Provide frequent and comprehensive communication and updates for employees and customers
- Clearly communicate testing protocols
- Update the general privacy notice or create a COVID specific privacy notice

4. Designate Single POC for Employees

- Designate a single POC to direct all questions, concerns, and complaints who can be entrusted with sensitive employee/personal information
- Define eligibility criteria for a referral to professional assistance (e.g., grief counseling)

10 Critical Actions to Take Now (cont.)

5. Adopt Specific Recordkeeping Protocols

- Limit recordkeeping to only suspected or confirmed cases
- Limit access to medical records, store separately from personnel records, and treat as highly confidential
- Destroy all relevant medical data following the pandemic

6. Limit Information Disclosed Internally and Externally

- Disclosures of the name of the impacted individual should only be made in three limited circumstances:
  - To health and safety government agencies without consent of the individual in cases of confirmed illness
  - To healthcare providers with consent of the individual to aid the individual's treatment
  - To family members with consent of the individual to help the family protect themselves and/or aid the individual's treatment

10 Critical Actions to Take Now (cont.)

7. Develop an Office Strategy

- Stagger employee returns
- Maintain social/physical distancing in the office (e.g., don't sit in cubicles next to each other)
- Require infection control practices (e.g., regular hand washing, PPE such as masks, discourage handshaking)
- Continue heightened cleaning, including all frequently touched surfaces
- Provide necessary supplies to employees (e.g., tissues, no-touch disposal receptacles, soap and water, hand sanitizers).
- Place posters that encourage good hygiene practices

8. Inform Employees about Remote Working Requirements for Data Protection

- Create complex passwords & maintain up-to-date security
- Enable router encryption
- Ensure adequate device protection
- Require employees to keep physical files secure
- Provide training and communication
- Wipe lost devices
- Rely on trusted networks and cloud services

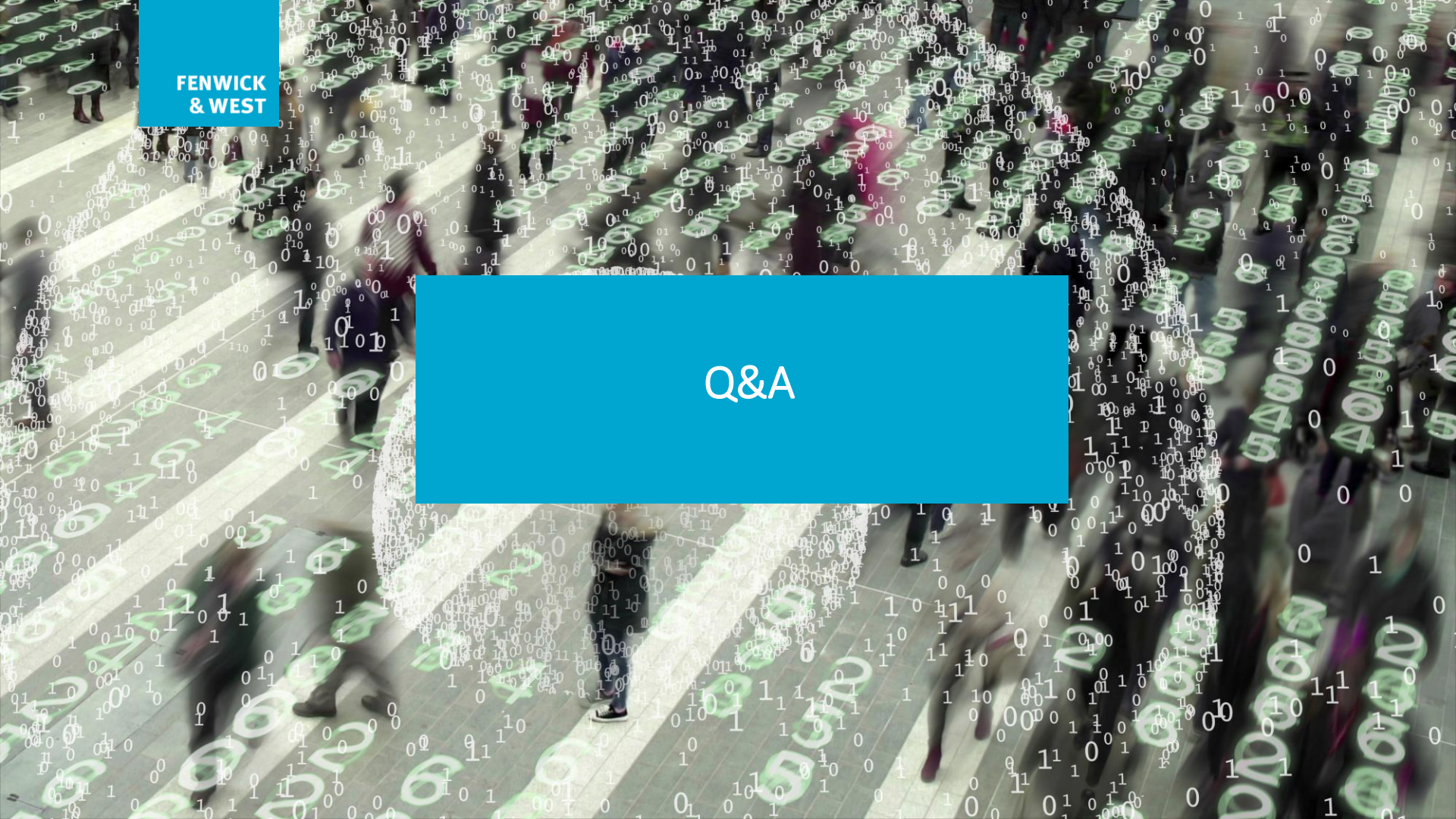
10 Critical Actions to Take Now (cont.)

9. Identify Control or Process Adjustments to Re-Evaluate Post-Pandemic

- E.g., subscriptions/memberships, access controls

10. Coordinate COVID-19 Information Handling and Disclosure Guidelines with Other Related Initiatives

- Recruiting and personnel challenges, including operating with a reduced workforce
- Executive team and employee travel policies
- Meeting protocol with potential customers, investors and others
- Company event and conference postponements and their impacts on your business
- Remote work and work-at-home policies
- Contract playbook on how to handle force majeure, amendments and performance guidelines
- Plans for infectious disease management
- Plans for conducting M&A and financing diligence remotely


FENWICK
& WEST
Q&A


FENWICK
& WEST
APPENDIX

COVID-19 Situation & HIPAA Requirements

OCR Recent Statements

- **February 2020 Bulletin: HIPAA and the Novel Coronavirus.** OCR provides guidance on disclosure of patient information during emergency situations.
- **March 2020 Notice of Enforcement Discretion.** OCR will waive potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies during the COVID-19 nationwide public health emergency.
- **Applicability**. HIPAA applies to Covered Entities (i.e., healthcare providers, health plans/payors, clearinghouses, as well as companies providing self-funded benefits) and Business Associates. There may be other state or federal rules that apply to the processing of medical information.

Permissible Disclosures

- **Balancing Health and Privacy**. HIPAA protects the privacy of patients' health information (Protected Health Information or PHI), but is balanced to ensure that appropriate uses and disclosures of the information still may be made when necessary (without patient authorization) for:
  - **Treatment**. To treat the patient or to treat a different patient. Treatment includes the coordination or management of healthcare and related services by one or more health care providers and others, consultation between providers, and the referral of patients for treatment.
  - **Public Health Activities**. To public health authorities, persons at-risk.
  - **Family, Friends, and Others Involved in an Individual's Care and for Notification**. To family members, relatives, friends, or other persons identified by the patient as involved in the patient's care.
  - **Serious and Imminent Threats**. To prevent or lessen a serious and imminent threat to the health and safety of a person or the public – consistent with applicable law (such as state statutes, regulations, or case law) and the provider's standards of ethical conduct.

Coordinate COVID-19 Information Handling and Disclosure Guidelines with Other Related Initiatives

Companies should keep in mind that privacy and health information collection and disclosure should be coordinated with other COVID-19 response efforts. The Fenwick COVID-19 Resource Center and team have been helping companies with important related initiatives that may have an impact on data security and privacy, including, but not limited to, the following:

- Health and safety guidelines for your office and employees
- Recruiting and personnel challenges, including operating with a reduced workforce
- Executive team and employee travel policies, including provisions for stranded travelers unable to return home
- Meeting protocol with potential customers, investors and others
- Policies in your global offices based on local health and data protection laws
- Company event and conference postponements and their impacts on your business
- Remote work and work-at-home policies
- Contract playbook on how to handle force majeure, amendments and performance guidelines
- Plans for infectious disease management
- Plans for conducting M&A and financing diligence remotely