

**AdvaMed Events & Education**

Webinar

# **COVID-19 Return to Work: Managing Safety, Data and Privacy for a Secure Workplace**

*August 13, 2020*

# COVID-19 Return to Work: Managing Safety, Data and Privacy for a Secure Workplace



*Hilary Wandall*

*SVP, Privacy Intelligence and General Counsel  
TrustArc*



*Andrew C. Fish*

*Chief Strategy Officer  
AdvaMed*

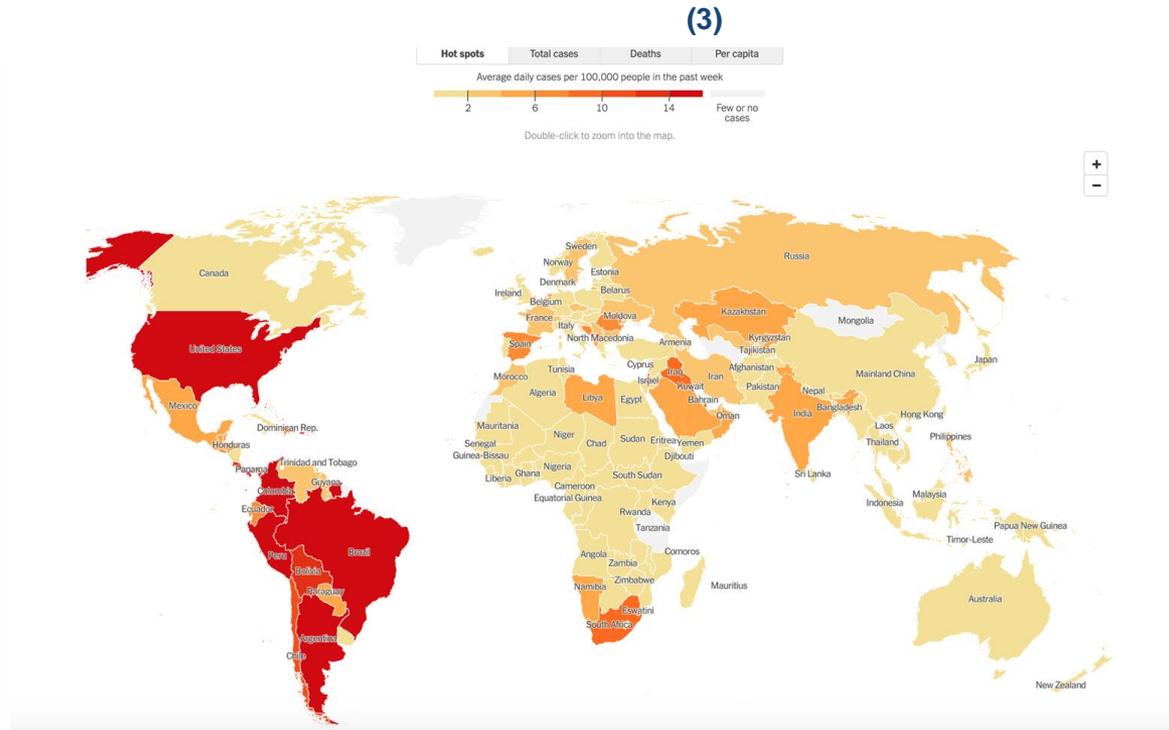
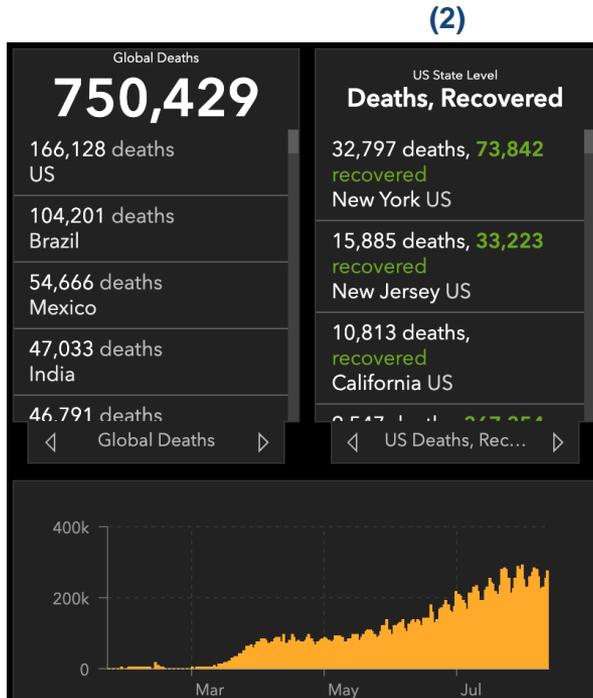


Managing Safety, Data, and Privacy  
for a Secure Workplace

C  VID-19

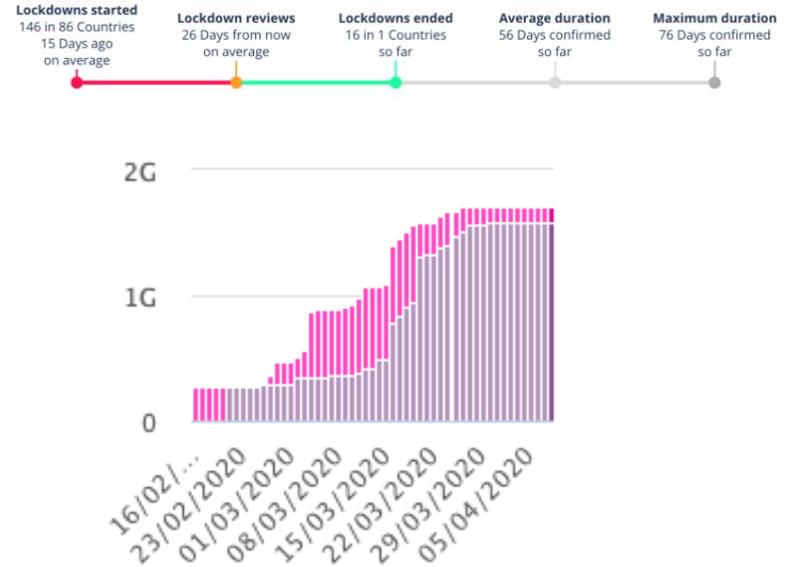
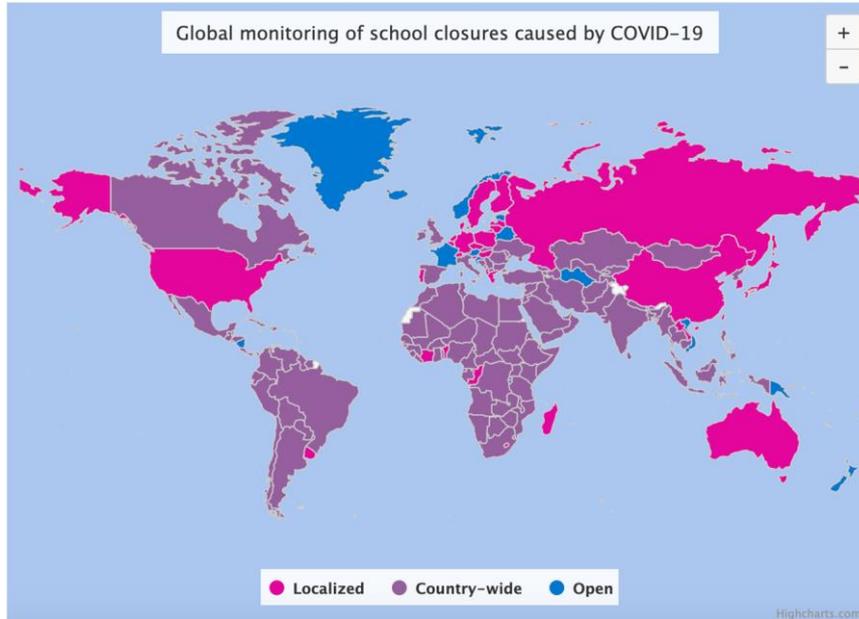
# Most disruptive pandemic in more than a century

- First known cases in early December 2019 in the Chinese city of Wuhan
- >20.6M cases reported in nearly every country<sup>(1)</sup>

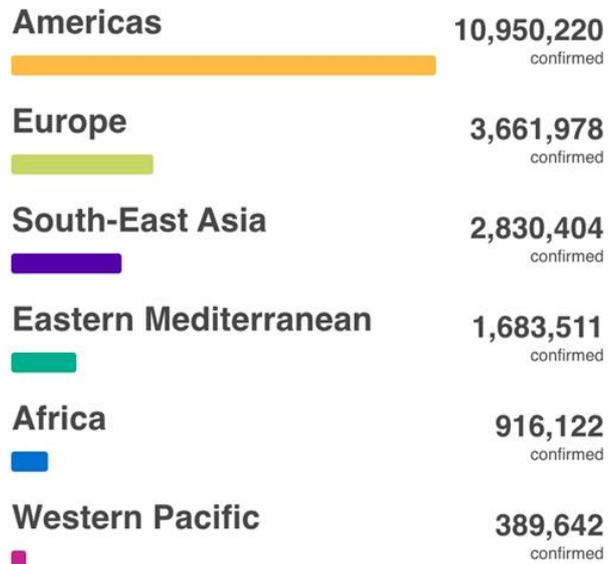


# Most disruptive pandemic in more than a century

- Over 80 Countries have had lockdowns, quarantines, or shelters in place<sup>(4)</sup>
- ~1.2 billion children are affected by school closures around the world<sup>(5)</sup>

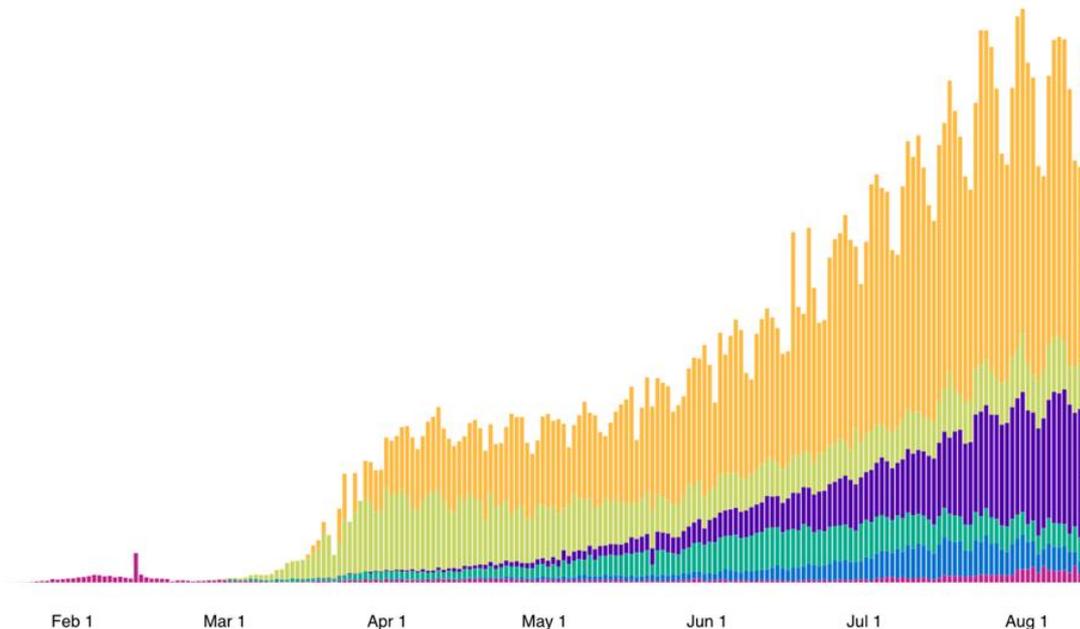


# A View Across Regions<sup>(6)</sup>



Source: World Health Organization

▨ Data may be incomplete for the current day or week.



# Reducing Transmission in the Workplace<sup>(7)</sup>

Less Expensive	More Expensive (and Invasive)
PPE and Masks	Daily questionnaires
Personal Hygiene	Contact-Tracing
Self-diagnosis	Testing
Physical distancing	
Redesigning Workspace	
Workspace cleaning	
Remote work	
Workforce segmentation	
Travel limitations	

# Over 100 Regulators Globally Have Provided Guidance<sup>(8)</sup>

Jurisdiction	Formal DPA/Regulator Guidance	Can We Collect Symptoms?	Can We Take Temperature Readings?	Can We Ask Employees to Notify of Diagnosis?	Can We Notify Other Staff?	Can We Notify Public Health Authorities?
 European Union	EDPB	●			●	
 Belgium	DPA	●	●	●	●	●
 Canada	OPC	●	●	●	●	●
 Denmark	DPA	●			●	
 France	CNIL	●	●	●		●
 Germany	DPA	●	●	●	●	●
 Ireland	DPC	●		●	●	
 Italy	DPA	●	●	●	●	●
 Netherlands	DPA	●	●	●	●	
 Spain	AEPD	●	●	●	●	●
 United Kingdom	ICO	●	●		●	
 United States	EEOC	●	●	●		●
 United States	CDC	●	●	●		●

## TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



- Can I require employees to return to the office?
- Can I require temperature screenings of all who enter our facilities?
- Can I require employees to use a contact tracing or exposure notification app?
- Can I require employees to report exposure?
- Can I require employees to report that they have been diagnosed?
- Can I require reporting that a member of the household has been diagnosed?
- What information can I share regarding an infected member of the workforce?
- How should I evaluate and control ongoing remote work data leakage risks?

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## Can I require employees to return to the office?

In the U.S., Canada, and the EU:

- Evaluate the business necessity for employees to return to the office and prioritize by role / function
- Mitigate the risk of imminent danger to employees - exposure risk to COVID-19 “direct threat”
- Classify jobs by exposure risk: very high, high, medium, low, very low (*most = lower exposure risk*)
- Undertake special considerations, including reasonable accommodations, for vulnerable populations
- Undertake special considerations for employees with caretaker obligations
- Consider implementing a screening checklist and/or protocol
- Update policies, data inventory, notices, and document privacy safeguards in a PIA

*TrustArc Research References:*

Employee Privacy: EEOC Additional Measures for Managing COVID-19

GDPR: EDPB Conditions for Processing COVID-19 Context

Employee Privacy: Measures for Canadian Employers to Manage COVID-19

DPA Israel Clarifies Return-to-Work Measures

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## Can I require temperature screenings of all who enter our facilities?

In the U.S., Canada, and the EU:

- According to the EEOC, during a pandemic employers may measure employees' body temperature
- In Lithuania, employers are not permitted to do temperature screenings
- Temperature readings are sensitive information and must be protected and safeguarded accordingly
- Obtain consent from visitors before conducting a temperature screening
- Establish data retention schedules that minimize storage to the shortest time needed (e.g., 24 hrs)
- Consider alternatives such as home temperature screens before employees come to work
- Update data inventories, privacy notices, provide training, and and document safeguards in a PIA

*TrustArc Research Reference:* COVID-19: Pennsylvania Health Department Best Practices for In-Person Businesses

*TrustArc Research Reference:* COVID-19: Employer Processing Obligations in Thailand

*TrustArc Research Reference:* COVID-19: DPA Lithuania Best Practices for Data Controllers

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## Can I require employees to use a contact tracing or exposure notification app?

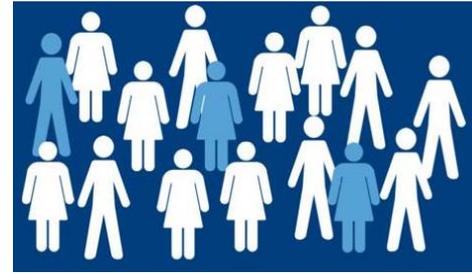
In the U.S., Canada, Asia, and the EU:

- Evaluate whether the country has adopted a centralized or decentralized approach to contact-tracing
- If no centralized approach exists in the country, consider employer-sponsored programs aimed at mitigating occupational health and safety risks, including technology-based programs where permitted by law and less intrusive programs cannot effectively mitigate the risk
- Avoid and/or minimize collecting or accessing data about personal activities unrelated to work
- If the app will also collect data from a healthcare provider or lab, ensure specific consent is obtained
- Ensure all data collected in the app is protected and safeguarded accordingly
- Ensure that the app provider has implemented effective Privacy by Design controls and look for independent review, audit, or certification of the effectiveness of those controls

*TrustArc Research Reference:* EDPB Measures for Use of Location and Contact Tracing Tools

*TrustArc Research Reference:* CoE and Convention 108 Joint Measures for Digital Contact Tracing

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## Can I require employees to report exposure?

In the U.S., Canada, Asia, and the EU:

- Determine if occupational health and safety law requires employees to report risks to the workplace
- Determine if emergency COVID-response measures require collection of contact history (e.g., if in contact with an exposed individual)
- Consider asking employees to contact occupational health care to evaluate the need for absence from work
- Provide employees a channel to report exposure in a secure and confidential manner
- The CDC requires health professionals to self-monitor and be evaluated by health authorities or occupational health program prior to returning to work

*TrustArc Research Reference: COVID-19: CDC Recommends Daily Screening of Healthcare Personnel*

*TrustArc Research Reference: COVID-19: NPC Philippines Best Practices for Processing Employee Personal Data*

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## Can I require employees to report that they have been diagnosed?

In the U.S., Canada, Asia, and the EU:

- Spain requires employees, management and safety workers to inform superiors of reported cases
- Assess if there is a legal basis for collecting health data (e.g., consent, public health)
- Consider what to do with confirmed reports (e.g., implement restrictions, disclose to health authorities)
- Consider asking employees to contact occupational health care to evaluate the need for absence from work
- Provide employees a channel to report infection in a secure and confidential manner

*TrustArc Research Reference: Employee Privacy: AEPD Spain Processing Conditions for COVID-19*  
*TrustArc Research Reference: Employee Privacy: Canadian Workplaces Can Collect Only Necessary COVID-19 Information*

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## Can I require reporting that a member of the household has been diagnosed?

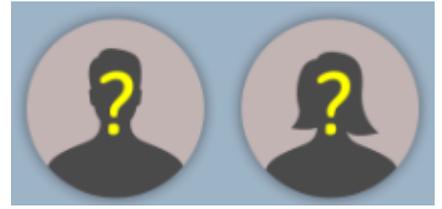
In the U.S., Canada, Asia, and the EU:

- In Germany, Latvia, and Lithuania would allow asking whether the employee has been in contact with an infected person.
- Disclosure of identity only permitted on exceptional basis (e.g., protect others with whom an infected person made contact)
- Data collected for pandemic purposes must be immediately deleted when pandemic is over

*TrustArc Research References:*

- *DPA Federal Germany Best Practices for Managing Coronavirus (COVID-19) in the Workplace*
- *COVID-19: Latvian DPA Processing Best Practices COVID-19:*
- *DPA Lithuania Best Practices for Data Controllers*

## TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



### What information can I share regarding an infected member of the workforce?

In the U.S., Canada, Asia, and the EU:

- Most jurisdictions permit disclosure that an employee has been infected, but prohibit disclosure of identifying information (e.g., name, occupation)
- Germany permits disclosure of the employee's identity only on an exceptional basis (e.g., to protect others with whom they have been in contact)
- Where permitted, disclosure can include number of days individual was present in the workplace, meetings they attended and community facilities used
- Determine if disclosure to health authorities would be more prudent than disclosure to employees
- Follow guidance from authorities on information to be included in public health disclosures

*TrustArc Research Reference: Sensitive Data: DPA Federal Germany Best Practices for Managing COVID-19 in the Workplace*

*TrustArc Research Reference: COVID-19: Pennsylvania Health Department Best Practices for In-Person Businesses*

# TrustArc Privacy Checklist for Enabling Companies to Reopen During the COVID-19 Pandemic



## How should I evaluate and control ongoing remote work data leakage risks?

In the U.S., Canada, Asia, and the EU:

- Develop remote work policies and make sure employees understand how to keep information private and secure, such as only working on work devices and not downloading local copies of information
- Update the acceptable use policy for work devices and tools, along with the use of personal devices
- Review and update basic security measures, such as anti-malware, software updates, VPN, etc.
- Develop a data health check process including:
  - Provide privacy & security training on returning to work, such as identifying work data stored outside approved locations, destroying data stored locally, and shredding paper copies
  - Review data processing activities to identify where sensitive data may have escaped due to alternative work streams and “emergency” vendors

*TrustArc Research References:*

*COVID-19: Uzbekistan Cyber Security Center Best Practices for Remote Working*

*Remote Access: ENISA Best Practices for Secure Home Connections*

# Top 10 Tips for Working Remotely<sup>(9)</sup>

## Managing Remote Workers

1. Remote Work Policy
2. Proper Tools, Apps, and Equipment
3. Incident Notifications and Security Concerns
4. Policies
5. Privacy Program Documents
6. Transparency
7. Privacy Laws
8. Other Laws
9. Manager Coordination
10. Health Insurance

## Enabling Remote Workers

1. Confidential Data Awareness
2. Proper Tools
3. Equipment Protection
4. Anti-malware and Patches
5. Passwords and Multi-factor Authentication
6. Limited Printing
7. Document Sharing and Storage
8. Work Devices
9. Personal Devices
10. Data Cleansing

# References

- (1) The New York Times. Coronavirus Map: Tracking the Global Outbreak.  
<https://www.nytimes.com/interactive/2020/world/coronavirus-maps.html>
- (2) Johns Hopkins University of Medicine. Coronavirus Resource Center.  
<https://coronavirus.jhu.edu/map.html>
- (3) The New York Times. Coronavirus Map: Tracking the Global Outbreak. Where Cases are Rising Fastest.  
<https://www.nytimes.com/interactive/2020/world/coronavirus-maps.html>
- (4) Aura Vision. Global COVID-19 Lockdown Tracker.  
<https://auravision.ai/covid19-lockdown-tracker/>
- (5) UNESCO. COVID-19 Educational Disruption and Response.  
<https://en.unesco.org/covid19/educationresponse>
- (6) WHO. Coronavirus (COVID-19). Case Comparison WHO Regions.  
<https://who.sprinklr.com/>
- (7) NEJM. Challenges of “Return to Work” in an Ongoing Pandemic. June 18, 2020. [nejm.org](https://www.nejm.org)
- (8) TrustArc Canada, Inc. Nymity Research and Alerts.  
<https://insights.nymity.com/search/trending/COVID-19>
- (9) TrustArc eBook. COVID-19 Privacy Risks and Considerations.

# COVID-19 Return to Work: Managing Safety, Data and Privacy for a Secure Workplace



***Hilary Wandall***  
***SVP, Privacy Intelligence and General Counsel***  
***TrustArc***



***Andrew C. Fish***  
***Chief Strategy Officer***  
***AdvaMed***

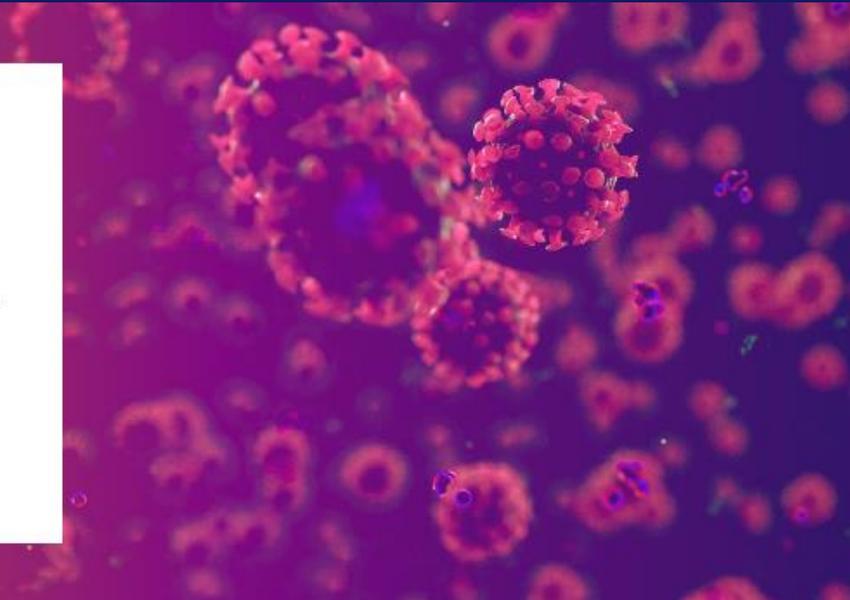


UNITED BY  
**PURPOSE**  
— UNITED BY MEDTECH —

THE VIRTUAL  
**MEDTECH**  
CONFERENCE

Powered by  AdvaMed

**ON DEMAND AND PARTNERING**  
**SEPT. 8 – OCT. 23, 2020**  
**LIVESTREAM**  
**OCTOBER 5 – 7, 2020**

A microscopic view of several COVID-19 virus particles, which are spherical and covered in small protrusions (spikes). The background is a dark, reddish-purple color with a bokeh effect of light spots.

# COVID-19 MEDTECH RESOURCE CENTER

**New Website Now Available!**

STAY CURRENT

**[MedtechResponds.com](https://www.MedtechResponds.com)**