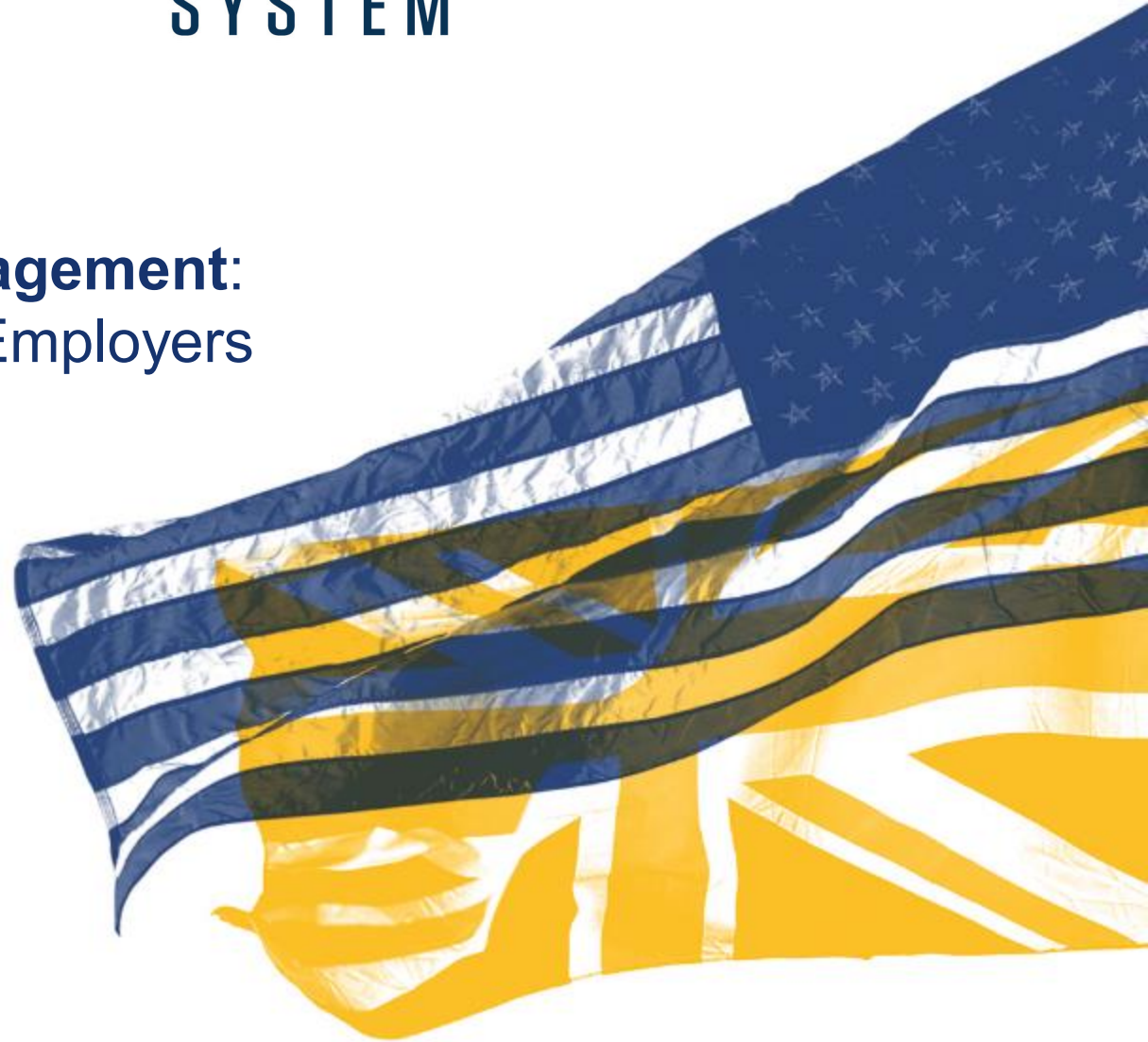


# COVID-19 Risk Management: Data Challenges for Employers

April 29, 2020



# Introductions

---



**Tara N. Cho, CIPP/U.S., CIPP/E**  
Partner, Womble Bond Dickinson

T: 919.755.8172  
E: tara.cho@wbd-us.com



**Theresa Sprain**  
Partner, Womble Bond Dickinson

T: 919.755.2104  
E: theresa.sprain@wbd-us.com

---



**L. Renee Williams, CIPP/U.S.**  
Senior Counsel, Harris Health  
System (HCAO)

T: 713.566.6554  
E: renee.lowe@harrishealth.org

# New Challenges and Competing Needs

---

- Urgency and uncertainty
- Getting the job done in a new way (at what cost?)
- Fast decisions and skewed judgment
- Unintended consequences / innocent mistakes
- Diminished or unpredictable resources and funding
- External stressors and new exposure points
- Ever-present bad actors seizing the opportunity
- Tensions between privacy and public health



# Meeting Competing Needs

- Employee privacy can collide with the need or desire for transparency
  - Co-worker Safety
  - Public health
- Economic crisis and need to continue operations (not a free-for-all on the pre-existing legal requirements)
- Record keeping is necessary for compliance with old and new laws
- Legal guidance is still evolving—be reasonable and document
- Security can be a major challenge for employers with a remote work environment



# Employee Privacy



# Medical Information

---

- Employee information vs. patient data vs. plan participant data
- What is medical information / what information is subject to HIPAA / what is / is not protected information (ADA, HIPAA, etc.)?
- HIPAA misconceptions
- Required disclosures / public health authorities
  - CDC-public health guidance on notifications
  - Public health overtaxed in making notifications
  - OSHA guidance on reporting
- Positive test results / suspected positive test results and employee privacy
- OCR waivers (first responders, business associates, etc.)

# Non- Discrimination and Retaliation

---

- Think about it in terms of your existing treatment of individuals with medical conditions
- Given the grave concern over COVID-19, there is potential for greater discrimination and/or retaliation for individuals who had or were perceived to have had COVID-19

# Employee Fraud

---

- Employees with fraudulent records
  - Increase in telehealth
  - Increase in available benefits





# Employee Temperature Testing

---

- Formerly an impermissible medical test according to the EEOC
- EEOC changed its guidance in March in response to the pandemic
- Now it is a recommendation from the CDC for essential workers who have been exposed
- There is very little guidance on how employers should do this from CDC or otherwise



# Recordkeeping

---

- Recordkeeping—is it necessary, and if so, how is it done?
- Think about whether a daily record is really necessary
  - If so, what is the purpose of keeping it?
  - If keeping it, what protections should be in place and for how long?



# Employee Monitoring

---

- After an employee is out of work, how are you monitoring activity and productivity?
- Do you need to track employees still at work?
- Google/Apple tracking apps



# Employee Privacy Notices

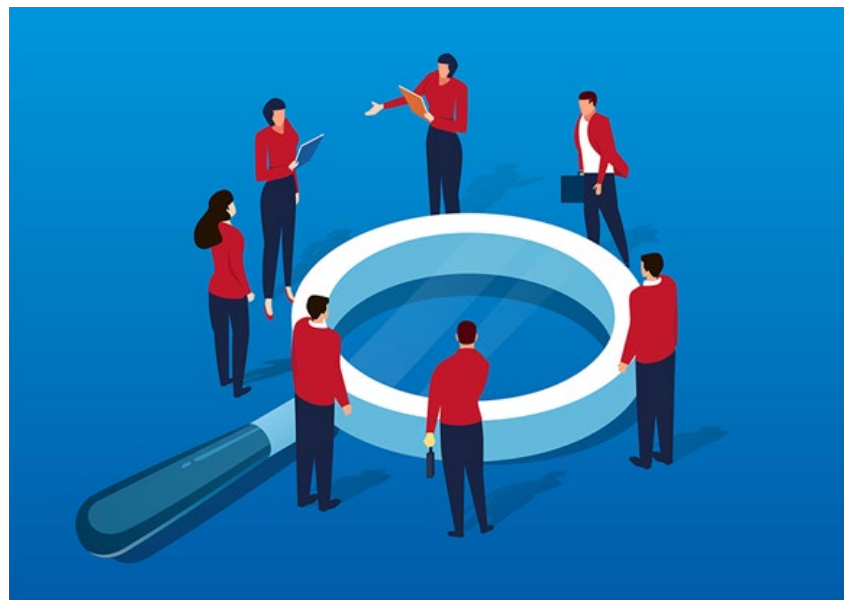
- What are you required to do?
- Do not forget state laws—  
California
- Consider the unintended  
consequence for not already  
being in compliance



# All Factors Have to Be Considered Together

---

- A corporate culture of transparency may not hold up to a pandemic
- The decision needs to be made early to avoid a perception of changing course
- Revealing too much—even a department—may identify individuals



# The New Workplace



# Business Continuity and Adaptability

---

- VPN and other remote network capabilities
- Availability of remote end user devices / equipment
- Load testing and backup
- Diminished resources and loss of funding

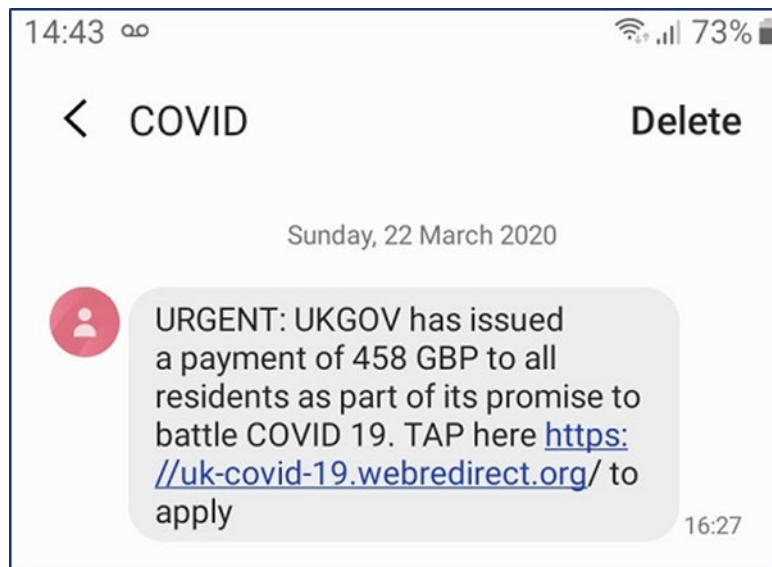






# Increased Cyber Attacks

Email and SMS text phishing and malware attacks using COVID-19 messaging as bait via emails asking recipient to visit a website, open an attachment, click a link or similar




Source: Alert (AA20-099A) from U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC) , April 8, 2020

# Increased Cyber Attacks

## Phishing Email Examples:

**COVID-19 Everything you need to know**

 • John DeFranco <[redacted]>  
To: [redacted]


How to Protect your friends from nCov 2019 FAQ


There are more than 75,000 infected COVID-19 cases all around the world!

[COVID-19-FAQ](#) - uploaded with iCloud Drive.

Regards,  
John DeFranco

**Coronavirus Update: China Operations** Wednesday, February 5, 2020 at 11:46 PM

 個人信箱 <sssmith44[redacted]>  
To: romio

 Factory Contacts an...  
43.4 KB

[Download All](#) [Preview All](#)

We would like to take a moment and ensure that our clients, partners, etc. are updated regarding the status of our operations in China.

Unfortunately, the New Year has been dominated by the 2019-nCoV (Coronavirus) outbreak. As of today, the number of confirmed cases has reached over 17,000, with over 300 deaths reported. We are monitoring the Johns Hopkins CSSE website that provides real-time data related to confirmed cases.

Wuhan (Hubei Province) is identified as the center of the outbreak and will remain under quarantine as the government continues with containment efforts. An increasing number of countries are now restricting visitors from this area, or China in general. Currently, more than 25 countries have confirmed cases.

Many companies, including manufacturers, in China are being asked to remain closed after the Lunar New Year holiday, through February 9th. We are among the organizations that will remain closed during this time and as advised. Please find attached our rescheduled resumption date including ways to contact our other factories outside China.

[redacted] remains proactive throughout the escalation of this virus. Two thousand masks from the U.S. were shipped to offices in China. Team chats are now in place to allow employees to check in and receive ongoing updates. We are grateful there are no cases of the Coronavirus affecting Pro QC employees at this time. Attached is also the approved ways by the WHO to avoid the virus.

We are asking our teams in the region to avoid crowded places as much as possible. And, we will continue to provide regular updates. We will work with the teams in China to continue managing operations from home starting February 3rd.

Please do not hesitate to contact your account manager or info@[redacted] for answers to questions, feedback, etc.

Source: Agio blog, March 19, 2020. <https://agio.com/newsroom/covid-19-malicious-domains-malware-phishing/>

# Increased Cyber Attacks

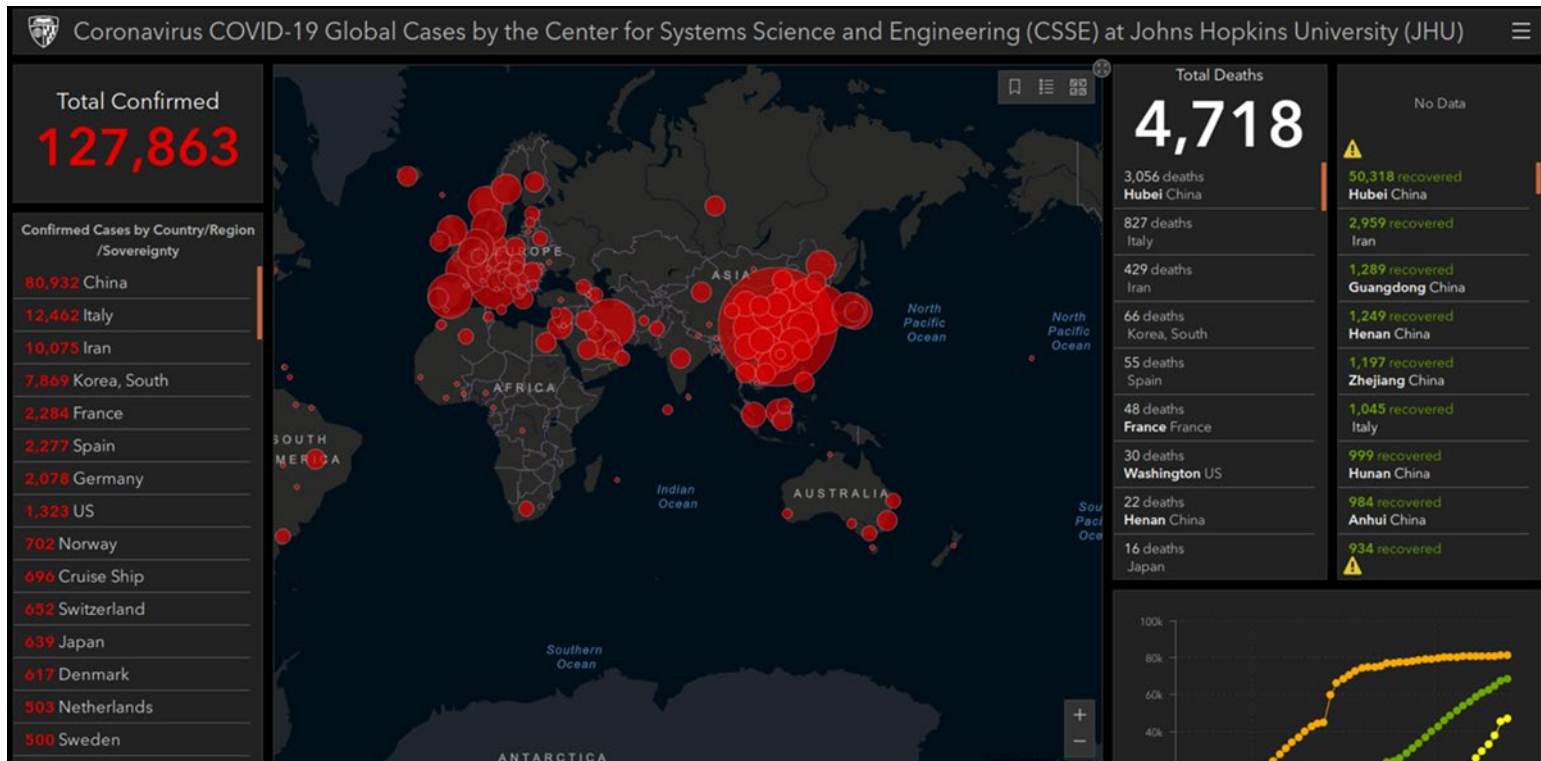
---

New domain names with COVID-19 related wording and fake sites that try to collect your personal information on sites that purport to provide:

- The latest COVID-19 new and updates in your area
- Outbreak tracking / positive cases in your location
- Info or customized details on tax or other financial benefits

# Increased Cyber Attacks

## Malicious Website Example:



Source: Krebs on Security, March 12, 2020.

<https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/>

# Increased Cyber Attacks

---

## Attacks on telecommuting infrastructure and vulnerabilities

- Unpatched software and other vulnerabilities
- Videoconference hijacking



# Other Types of Fraud and Scams

---

Other forms of misconduct emerging

- Fake charities
- Snooping employees



# Life After COVID-19: Return to Work



# What Happens with the Data?

---

What should you do with the data amassed during the crisis?

- Some employee records will still be necessary for compliance purposes—tax credits for emergency leave, workers compensation claims, ongoing leave needs
- What can I delete?
- Consideration of record retention laws and policies





# Employees Who Want to Continue to Work Remotely or Refuse to Return to Work

---

- NLRA/OSHA rights
- ADA accommodation to work from home?
- What physical measures/steps have been improved that might allow remote work where not allowed before?
- What have you learned about security that makes this not possible?

# Returning Your Data to Work

- Transitioning the data from crisis mode/personal devices to normal operations and policies
- Start now to inventory who has this and what types of material
- Separating business from personal may be something employee does not want employer to do—how do we confirm?
- Certifications by employee



# Transitioning to longer-term remote work

---

- If you're going long-term remote workforce, have you really fully vetted security aspects vs. band-aid?
- What policies are already in place?
  1. Revisit BYOD and WFH policies
  2. Some already revised in this time period to confirm use of BYOD/remind of confidentiality obligations
- What technology solutions do you need?
- Tracking devices and equipment
- Are there limits on remote access now that it is more ongoing?



# Questions?



# Our Speakers

---



**Tara N. Cho, CIPP/U.S., CIPP/E**  
Partner, Womble Bond Dickinson

T: 919.755.8172  
E: tara.cho@wbd-us.com



**Theresa Sprain**  
Partner, Womble Bond Dickinson

T: 919.755.2104  
E: theresa.sprain@wbd-us.com



**L. Renee Williams, CIPP/U.S.**  
Senior Counsel, Harris Health  
System (HCAO)

T: 713.566.6554  
E: renee.lowe@harrishealth.org