Privacy in a Pandemic

Discussion of privacy issues during the COVID-19 pandemic

WINSTON & STRAWN LLP

Speakers

Sheryl Falk

Partner, Houston
sfalk@Winston.com

Aviva Grumet-Morris

Partner, Chicago
agmorris@Winston.com

Alessandra Swanson

Partner, Chicago
aswanson@Winston.com

Privacy Challenges

State & Federal Privacy Law Guidance	▪ Remote work force ▪ CCPA enforcement ▪ HIPAA guidance
Employee Privacy	▪ Informing employees about COVID-19 diagnoses ▪ Employer obligations regarding confidentiality ▪ Employer actions toward protecting the workplace
Data Security Issues	▪ Remote work force data security ▪ Secure virtual meeting applications ▪ Cyber-attack prevention & response

WINSTON & STRAWN LLP

Complying with State & Federal Privacy Law

Alessandra Swanson

Question 1

- Q: My company had to quickly transition our entire workforce to telework. Now that we have transitioned to our “new normal,” what steps can we take to ensure we are meeting our privacy obligations?

- A. Take a multi-prong approach to ensure that your employees understand their obligations.
  - Review key policies, include information handling procedures and “bring your own device” policies.
  - Ensure employees know how to communicate with one another, now that they can’t just walk down the hallway to talk to co-workers.
  - Keep an eye out for regulatory guidance; HHS, EEOC and others are constantly communicating updates about how to interpret privacy obligations in the wake of the pandemic, and this will impact your organization’s strategy.

Question 2

- Q: Have there been any indications that enforcement of new state privacy laws will be delayed?

- A. No.
  - The NY SHIELD Act and CCPA went into effect this year, but there is no indication that enforcement of either law will be delayed. In mid-March, California Attorney General's office stated that it was moving forward with finalizing the regulations and enforcing the law.
  - As a practical matter, privacy enforcement is likely a low priority of Attorneys General at the moment.
  - To the extent possible given the pandemic, understand where compliance measures stand and make a plan to proceed, prioritizing the items that can create the highest risk to organizations (e.g., data security).

Question 3

- Q: Does HIPAA impact what my company can disclose about individuals at my company who have been diagnosed with COVID-19?

- A. Probably not.
  - Employers are generally not required to comply with HIPAA.
  - That stated, self-insured employer-sponsored health plans are covered entities, and may only disclose protected health information as permitted or required by HIPAA.
  - While HIPAA may not impact the employer's ability to disclose the information, there may be various state and federal laws and regulations that protect employee privacy which could prohibit the employer from disclosing the information

WINSTON & STRAWN LLP

Employee Privacy Questions

Aviva Grumet-Morris

First, Some Background…

- The Americans with Disabilities Act (ADA) governs an employer's interactions with both job applicants and employees in a number of ways, including:
  - Regulating "disability-related inquiries" and "medical examinations" of job applicants and employees.
  - Requiring employers to maintain the confidentiality of medical information.

Question 1

- Q. What if an employee exhibits symptoms of COVID-19, but has not been tested and wants to return to work?
- A. Employers can ask employees entering the workplace about symptoms and can exclude symptomatic employees from the workplace as a direct threat.

Question 2

- Q. What happens if my employee tests positive for COVID-19 – can I tell other employees?
- A. Yes, but:
  - Must maintain confidentiality – cannot reveal the identity of the sick employee.
  - All information regarding a medical condition or medical history of an employee must be maintained on **separate forms** and in **separate medical files** and be **treated as a confidential medical record**.

Question 3

- Q. An employee tested positive. The employer contacted the employees that the sick employee had direct contact with and informed them of the positive diagnosis of "an employee." The employee has since posted on social media that she had the virus, and now all of the other employees are questioning why the employer didn't inform them of the individual's identity. What is the proper way to address this issue?
- A. The fact that an employee self-identifies does not change an employer's obligation to maintain confidentiality.
- A. Consider discussing confidentiality – generally – with employees and steps taken in response to report of a sick employee.

Question 4

- Q: A supervisor learns that an employee's in-law passes away. The supervisor does not know the cause of death. The supervisor wants to ask the employee if the in-law died as a result of COVID-19. Is that permitted? If the supervisor finds out the death is COVID-19 related, can the supervisor request that the employee stay home to monitor him/herself for symptoms and go to the doctor?
- A. Unclear based on the facts presented.
  - Is the employee teleworking or coming into the workplace?
  - Any reason to think death of in-law was from COVID-19?
  - Any reason to think employee had contact with relative before death while contagious?

WINSTON & STRAWN LLP

Data Security Challenges

Sheryl Falk

Question 1

- Q: What data security best practices should companies use for remote workforce?

- A. It's more important than ever to work with employees on data security.
  - Require secure connections/VPN
  - Use two-factor authentication to access company data
  - Use pre-approved file sharing methods that have been confirmed as secure
  - Partner with employees on patching/updating anti-virus/malware
  - Limit employee access to data based on job role
  - Communicate with employees on data handling expectations

Question 2

- Q: Is it safe to use Zoom, Microsoft Teams, or other third party communication applications?

- A. Vet new applications/platforms
  - Communicate with employees about using only approved virtual meeting services
  - Issue unique PINS or passwords for each attendee
  - Use a “green room” and don’t allow meeting to start before the host
  - Lock the call once you have identified the attendees
  - Lock down the ability of the attendees to share the screen
  - Remind users not to share sensitive information
  - Only conduct meetings on company issued devices

Question 3

- Q: What can companies do to reduce the chance of a cyberattack?

- A. Be proactive. Be vigilant.
  - Re-circulate written information security plan to employees
  - Be on guard for phishing emails (fake COVID-19 alerts, CDC, etc.)
  - Communicate with employees about how to report suspicious activity
  - Monitor for unusual spikes in external network activity
  - Dust off your cyber plan
  - Maintain off-channel ways to communicate with your response team

Thank you for joining us today

Sheryl Falk

Partner, Houston
sfalk@Winston.com

Aviva Grumet-Morris

Partner, Chicago
agmorris@Winston.com

Alessandra Swanson

Partner, Chicago
aswanson@Winston.com

WINSTON
& STRAWN
LLP