



Jul 27, 2020

Categories:

[Blogs](#)

[Technology Blog](#)

Privacy Considerations During the Coronavirus Pandemic

Be Smart

The pandemic has forced many more employees to work from home. While working remotely provides some logistical advantages and allows us to respect social distancing guidelines, it also presents risks to our personal privacy and to the confidentiality and security of business information. The following is a list of issues and recommendations to consider when it comes to privacy and data security during COVID-19:

Cybersecurity for Remote Workforces

Issues:

- Employees accessing the company's systems remotely without using virtual private networks (VPNs) or properly configured firewalls may violate the company's internal information security policies or its contractual obligations related to transfers and storage of information and compliance with international privacy rules.
- Information may be accessed by unauthorized parties (e.g., a "family" computer used by other members of a household)
- Sharing files or information through online tools that are not approved by the company or that have been downloaded onto company-issued devices may violate the company's data retention and destruction policies.

Recommendations:

- Ensure that your Incident Response Plan is updated, has been tested, and can be readily deployed when your employees are working remotely.

- Update VPNs, network infrastructure devices, and devices being used to log in remotely to work environments with the latest software patches and security configurations.
- Remind employees of your company's information security, data handling, BYOD (bring your own device), data classification and data destruction requirements.
- Ensure IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
- Implement multifactor authentication on all VPN connections.
- Test capacity for remote access solutions.
- Make sure that clear and up-to-date policies for working remotely are provided to employees, especially those using video conferencing tools.

Social Engineering Attacks and Data Breaches

Issues:

- There has been a reported increase in phishing scams through emails pretending to be from the IRS or the CDC, as well as scams related to receiving financial stimulus and links for donations.
- Awareness about cybersecurity is not top of mind for employees when working from home.

Recommendation:

- Alert employees about social engineering attacks and offer training refreshers on how to detect and report phishing attacks.

Privacy of Employee Information

Issue:

- Employers are not sure what information may be requested from an employee who calls in sick. Can they assess and log

employee symptoms at work? Can they disclose the identity of an employee with COVID-19?

Recommendations:

- Limit the collection of, and access to, employee medical data to the minimum necessary to carry out the company's obligations.
- Consult guides from agencies about the confidentiality and collection of employees' information during COVID-19, including recent guidance from the Equal Employment Opportunity Commission, the Department of Health and Human Services, and the Department of Labor.
- Keep in mind that previously enacted privacy and data security regulations are still enforceable during COVID-19. The Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), the California Consumer Privacy Act (CCPA) and other laws that protect the privacy of individuals must still be followed during the pandemic. While many of the issues and recommendations outlined above apply to businesses under normal circumstances, the recent rapid transition to remote operations has only increased the importance of instituting effective privacy and data security practices.

For questions and assistance regarding this topic, please feel free to contact any member of our [Privacy and Data Security Team](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.