Top 10 Tips for Companies with (new) Remote Workers

More likely than not, especially if you are reading this, your company has taken the step to require or allow a remote workforce. It may seem relatively easy to do so - they all have computers. It’s not quite that simple. We have listed our top ten tips below that provide a solid foundation to start (or improve) your remote work policies and practices.

1. Remote Work Policy
   Develop and / or review your work from home policy to include elements arising during the current time. Refer to the Section I on top 10 tips for remote employees. All employers should have such a policy, even if remote work is only permitted for executives or in unusual circumstances. If employees can check email remotely – they are working remotely.

2. Proper Tools, Apps, and Equipment
   IT should make sure VPN can handle additional workload, especially for legacy systems and applications that are not cloud-based. Check subscriptions to common apps to make sure they meet the enterprise privacy and security requirements. For example, if you are subject to HIPAA, do you have the licenses on cloud services – platforms, software – to address regulatory privacy and security requirements for additional workers who would normally only work in the controlled environment.

3. Incident Notification and Security Concerns
   All employees should have the contact name, number, and email for security concerns in their phones and / or location other than their standard work device. Remind employees about confidential data handling protocols and provide security reminders for phishing, etc. Refresh employees on privacy and security measures and incident reporting requirements. Also, conduct a remote mock incident response. In addition, SANS came out with a remote work toolkit [here](#).

4. Policies
   Review your corporate incident response, business continuity, and disaster recovery policies and procedures in light of the current circumstances. Update them as required. Review associated policies, such as data classification, retention, and destruction.

5. Privacy Program Documents
   Review your records of processing activities and / or data inventories to make sure applicable processes are captured and updated. The processes of identifying at risk employees, infected employees, travel allowances, etc. may qualify as high risk processes. Likely, the processes involve sensitive personal data. Being sick or at risk is health data, being exposed through travel or other people may not be.

6. Transparency
   Various privacy laws require transparency around the personal data being collected and sharing how the data is collected and shared. If you are changing your practices about what data you collect on your employees, you should review your privacy notices to make sure that data is covered or added – especially if you are using data collected in one context for another. If your policies are updated, please also inform relevant stakeholders of the changes and the date these become effective.

7. Privacy Laws
   Most countries seem to have privacy policies now, along with some states and sectors in the US. Make sure you stay abreast of privacy guidance issued by regulatory authorities, especially in such locations as the EU. Yes, the European Union's General Data Protection Regulation may have allowances for emergencies and necessary data (see Article 6 and Recital 46), but it’s not a free ticket to ignore all data processing requirements. For example, check out this resource by Baker-McKenzie [here](#), which includes information on whether you can check temperatures of employees and visitors, require employees to inform managers of symptoms, and whether or not the applicable regulators have issued guidance. Some other resources include:
   - The Norwegian Supervisory Authority [issued guidance](#).
   - GDPR Article 6 and Recital 46 address the needs to collect data to protect others. See IAPP [article](#).
   - China, Hong Kong, and Singapore released advisories on privacy of employee data [here](#).

8. Other Laws
   There are also employment and discrimination laws and occupational safety laws that apply to the current circumstances, such as disability rights, civil rights, and refusal to work. Many of these laws have privacy elements to them, such as implicating personal data that may be sensitive. Make sure you stay abreast of advisories and guidance being issued by legal authorities as well as reputable law firms. This guide by Fisher Phillips is extensive and being updated regularly [here](#).

9. Manager Coordination
   Managers should know how to reach employees in an emergency and employees should know how to reach their managers. Managers should know how to identify signs of illness and what to do, as well as know what to do for employees who are at risk themselves or lives with someone who is at risk (elderly or immunocompromised) without violating privacy laws or creating employment issues. Genetic information, which includes relatives or the employee with no genetic information, may be sensitive. Make sure you stay abreast of advisories and guidance being issued by legal authorities as well as reputable law firms. This guide by Fisher Phillips is extensive and being updated regularly [here](#).

10. Health Insurance
    There are various concerns around health insurance, coverage, co-pays for hourly employees who may not be able to work, and other topics. Employers have a variety of options to choose from but should maintain awareness of how the data collected in these circumstances can and should be used. Some companies are self-insured and may have even more concerns about how to manage personal data. See this resource from Jackson Lewis [here](#).

Last, remember that although there may be some latitude in actions you can take with personal data during unexpected circumstances, not all unexpected actions are emergencies. Each of the tips above is something that can be addressed in advance as well as used as guidance for unexpected situations. Whenever you have doubts about a legal requirement, check with your attorney for advice.