Privacy Compliance and Remote Work

Technology has kept businesses afloat over the past year. However, moving millions of employees to work from home comes on the heels of a growing global focus on data privacy. Consequently, organizations already scrambling to meet regulations now face the dilemma of supporting both privacy compliance and remote work.

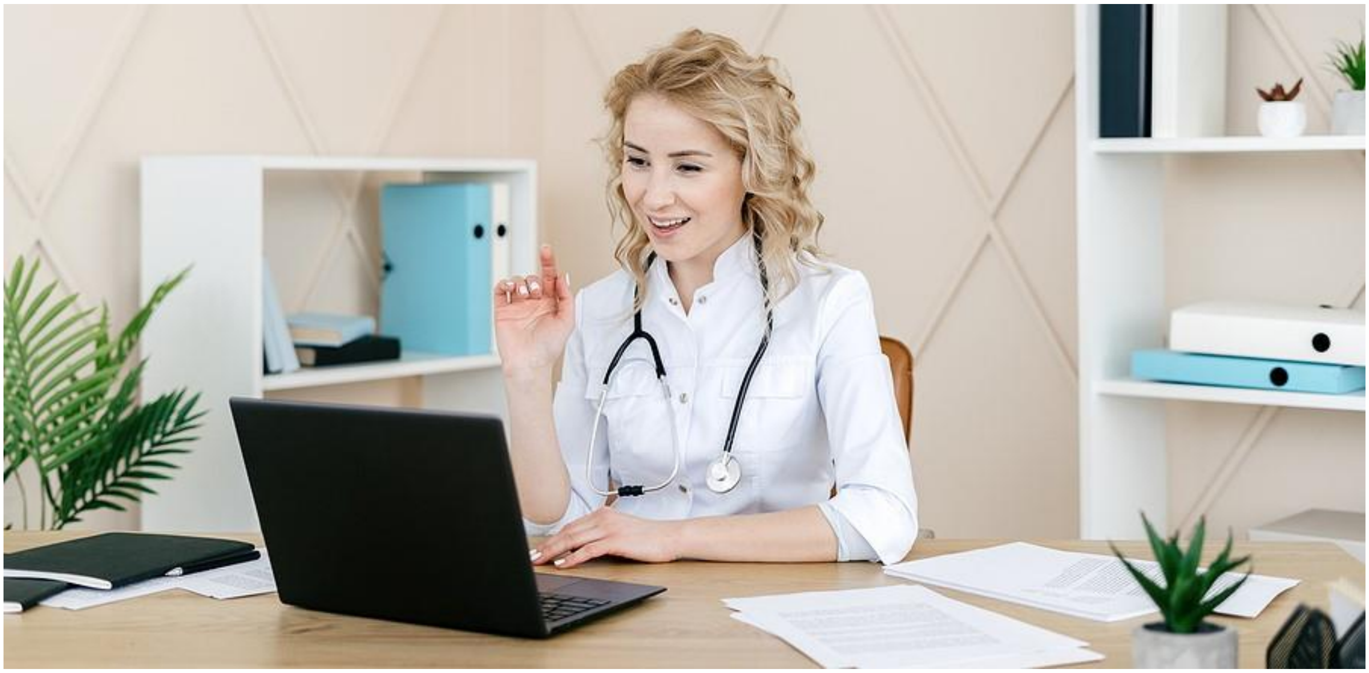
Consider several typical scenarios. Employees work on personal devices more than ever before, devices that may lack up-to-date security measures and secure Wi-Fi. Medical professionals conduct patient visits over video. Roommates and families share home networks and office space.

Employees and organizations alike must take responsibility for privacy compliance and data security. This begins with understanding the risks and the regulations involved. Then, both individuals and companies need to implement best practices to minimize those risks.

Common Privacy Compliance and Remote Work Challenges

Remote work brings inherent privacy and security risks. Controlling access to sensitive data tops the list. For instance, healthcare professionals working remotely must comply with HIPAA regulations regarding safeguarding personal health information (PHI). Yet they often work surrounded by family members who might accidentally see or hear privileged information.

Protecting sensitive data becomes even more difficult when employees use personal devices for work. Personal devices typically lack the security measures of corporate-controlled devices and thus will prove more susceptible to malware. Additionally, the use of personal devices complicates adherence to document retention and disposal regulations.



Outside the safety net of the office, the responsibility for security and privacy rests on the individual employee. The checks and balances built into office systems prove more difficult to implement in remote work. And without adequate tools and training, employees can unwittingly put the organization at risk of noncompliance and data breach.

Organization Best Practices

Organizations must adjust security practices to reflect the evolving challenges of remote work. Begin by conducting a compliance risk assessment. Understand the data landscape, including evolving workflows and endpoints. Then update security and privacy policies accordingly. This will certainly include any BYOD and password policies, as well as remote access protocols.

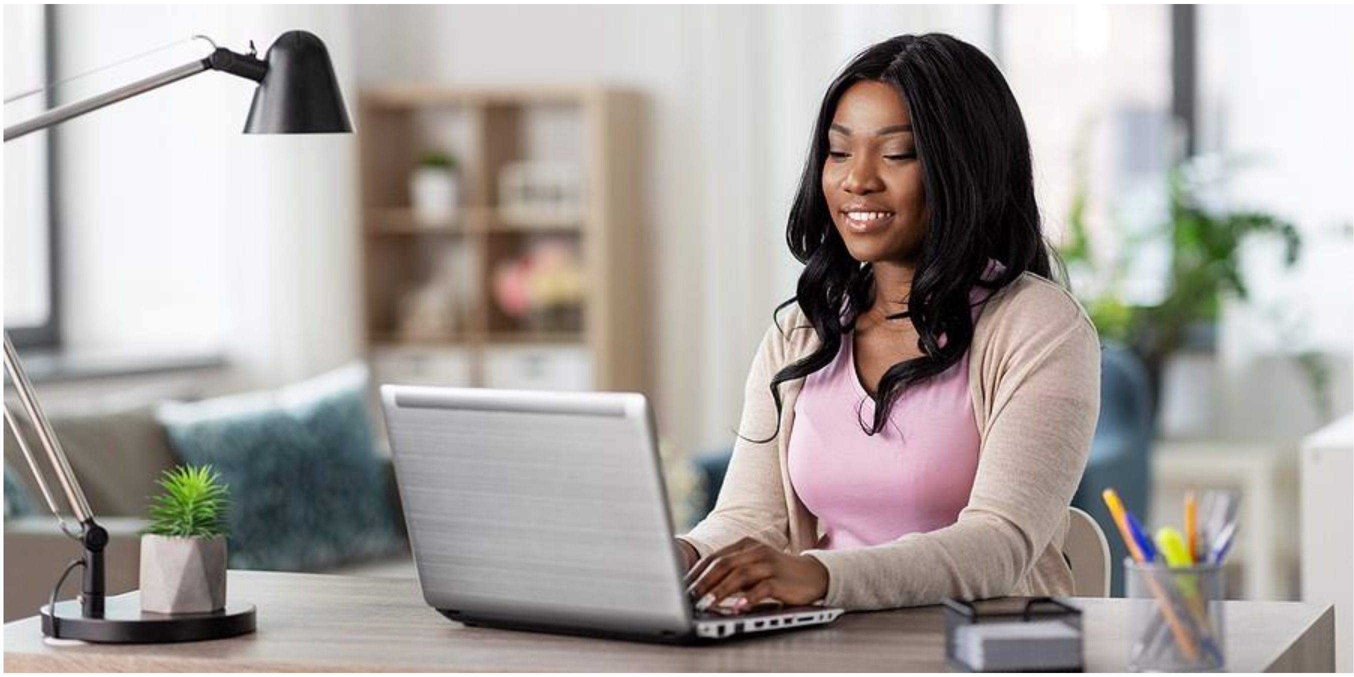
Ensure that employees have both the technology and the training that they need to comply with security and privacy protocols. This may involve one-on-one assistance to implement security measures. And it will definitely include regular and multi-faceted employee education.

Assess your networks and access controls and update as necessary. For instance, the VPN that served a handful of remote employees well may crumble under the demand of hundreds of remote employees. Additionally, utilize mobile device management (MDM) as a vital part of endpoint security.

Employee Best Practices to Promote Compliance

Organizations can, and should, implement robust security measures to protect networks and secure endpoints. But individual employees fill a key role in achieving compliance with privacy regulations. Essential best practices for remote workers include the following:

- Secure all devices used for work – This includes applying password protections and encryption on each device, including mobile devices and laptops. Keep devices in a safe location and lock them when not in use. Apply necessary updates such as operating system and antivirus.



- Passwords and MFA – Follow established guidelines for strong passwords. Use multi-factor authentication (MFA) when possible. Be sure to change the default password to the wireless router.
- Encryption and data transfer – Never transmit sensitive data without encryption. Additionally, follow established security policies for data transfer. In addition to email and file sharing policies, this includes using only approved devices when copying data to external media.
- Follow security policies for remote access – Never use public Wi-Fi for work. Ideally, use a secure VPN connection.
- Know how to recognize scams – Practice safe computing. Know the signs of a phishing scam and be vigilant. Never click links or open files from an unverified source. Confirm all requests for sensitive or personal information.
- Safe video calling – When conducting or attending a video meeting, understand and use the privacy settings available. For instance, use passcodes to restrict meetings to invited attendees.

Partner with Compliance Experts

Remote work complicates an already complex regulatory landscape. The compliance and security experts at Messaging Architects can help you secure your business and achieve compliance. From initial risk assessment to implementing multi-faceted data security and conducting ongoing data compliance monitoring, we have you covered.