STRATEGIC MANAGEMENT SERVICES

2023 Updated DOJ Compliance Guidelines Regarding Personal/Communication Devices, Platforms and Messaging Applications

Richard P. Kusserow | March 2023

Key Points:

- **New focus of updated DOJ "Evaluation of Corporate Compliance Programs."**
- **Tips for Compliance Officers**

In March 2023, DOJ released updated guidance that included how it will consider corporate practices addressing use of personal devices, messaging applications, and communications platforms in the workplace. The DOJ expects organizations to maintain, communicate and enforce policies that ensure that "business-related electronic data and communications can be preserved and accessed." If companies fail to do so, the DOJ will take this into consideration when settling cases. As part of this update to DOJ's "Evaluation of Corporate Compliance Programs (ECCP)," prosecutors will evaluate a corporation's policies governing electronic devices and data against the backdrop of the company's risk profile, and specific business needs when assessing the organization's ability to access and preserve electronic data and communications. In conducting this evaluation, prosecutors are directed to consider three factors:

1. **Communication Channels.** DOJ has emphasized focusing on electronic communications channels used by an organization and its employees and controls that manage and preserve information within those channels.
2. **Policy Environment.** Prosecutors will examine the policies that secure, monitor and access business-related communications. If "bring your own device" (BYOD) is permitted, they will question whether there are policies for preserving and accessing data and communications on them. There is also the matter of whether the organization is enforcing the policies.
3. **Risk Management.** A major focus is on organization management of security and controls over company data and communications. Prosecutors will examine the organization's

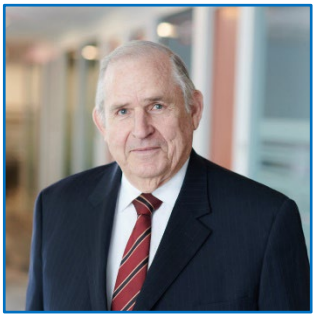
controls in managing communication channels, including personal devices or messaging applications, and whether these channels block or inhibit Compliance Officers from conducting internal investigations or responding to requests from enforcement or regulatory agencies.

Tips for Compliance Officers

- Determine the organization's policy concerning BYOD in the workplace.
- Evaluate policies regarding the permissible use of mobile devices and third-party messaging applications to ensure meeting regulatory record-keeping requirements.
- Ensure employees receive periodic training on the permissible-use policies.
- Conduct regular monitoring of communications for compliance with applicable policies.
- Take immediate action on identified non-compliance with communication and messaging policies and controls.
- Ensure communications channels and disciplinary policies are publicized and readily available to employees.

For answers to compliance FAQs, see https://www.compliance.com/faqs/

Keep up-to-date with Strategic Management Services by following us on LinkedIn.



About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.