ANALYST CONNECTION
Sponsored by: T-Mobile for Business

Mobile communications has become a critical tool for organizations, and its use should be managed accordingly.

Navigating Compliance Solutions for Communications in Regulated Organizations

October 2022

Questions posed by: T-Mobile for Business

Answers by: Jason Leigh, Research Manager, 5G and Mobile Services, and Sandra Wendelken, Senior Research Analyst, Mobile and IoT Services

Q. How are recent changes in the regulatory landscape impacting mobile device usage and monitoring within organizations?

A. It's not so much that the regulatory landscape is changing; rather, it's a broader acknowledgement of the pervasive role that digital mobile communications plays in day-to-day business life. Mobile communications must be included in the scope of rules that have traditionally applied to hardcopy files. While this may seem "new," the scrutiny of digital communications has been going on for more than 20 years, perhaps most famously in 2002 when the Department of Justice leveraged Microsoft internal emails in its antitrust case.

Today, nearly every regulated industry, and many self-governing bodies, include requirements for recording and archiving digital communications. But many of those rules were developed before text and instant messaging services on the smartphone were ubiquitous. Regulations around the capture and archiving of employees' work-related communications, even those that happen outside official, company-deployed tools, are still evolving. The National Futures Association (NFA) requires member firms have policies for monitoring phone calls and capturing SMS messages. Failure to comply with those rules can result in fines and suspension/censure of firms and individual employees.

In healthcare, while the rules around the Health Insurance Portability and Accountability Act (HIPAA) don't specifically address text messaging, they do require that a patient's personal health information (PHI) be encrypted at a minimum. With many medical professionals using personal mobile devices when on call, ensuring PHI compliance can be problematic. And the legal industry has always been keen on digital record-keeping, with a wide range of ediscovery solutions available. But as lawyers increasingly communicate with clients and each other via text messaging, internal compliance and record-keeping with these newer digital tools would benefit from new solutions for mobile devices.

Q. Why should organizations prioritize more rigorous oversight of their mobile communications?

A. There is a casualness with which most people approach electronic communications. Employees can regard text and instant message communications as "unofficial." And they tend to be less rigorous in reviewing the content of and complying with the retention of mobile messaging. This can be particularly true with the widespread use of bring-your-own-device (BYOD) programs among many organizations. Combined with the rapid expansion of hybrid work in the past couple of years, the lines between personal and business communications have blurred substantially, exposing organizations to compliance risk.

The most obvious reason to prioritize robust mobile compliance solutions is the financial one. A laissez-faire approach to monitoring, capturing, and archiving can result in hefty fines from regulators and other bodies for failing to comply with communications record-keeping requirements. Willful disregard of HIPAA rules, which cover text and instant messaging, can result in fines ranging from $12,000 to $63,000 per violation, up to a cumulative per-year maximum of more than $1.9 million. Broker-dealers have been hit with $100,000 fines and employee suspensions for violating record-keeping provisions. The SEC is suspected to have levied over $1 billion in penalties against financial institutions that failed to monitor use of unauthorized messaging apps.

Even if a company is facing a lawsuit or regulatory investigation, having detailed communications compliance policies and technologies in place can demonstrate the company's good faith effort to ensure compliance. This can be a mitigating factor in determining noncompliance penalties. Much like driving a car with an alarm system, taking a rigorous approach to communications compliance can lead to lower risk management insurance premiums.

Q. How can mobile compliance solutions for employees automate regulatory requirements and provide value to organizations?

A. The old adage that employees are the first line of defense in cybersecurity holds true for managing mobile communications as well. Organizations should provide their employees with proper guidelines to ensure they are aware of their role in regulatory data compliance, in safeguarding critical and private data, and in the appropriate use of mobile devices.

But policies are just the start. Technology tools are indispensable in ensuring compliance, mitigating organizational risk, and driving additional insights. Mobile compliance solutions provide a layer of protection against employees trying to skirt documentation requirements through voice and text/instant messaging usage. While technology does not provide an absolute guarantee, deploying robust compliance tools can demonstrate a genuine effort to adhere to regulatory requirements, which can provide some mitigation in the event of an investigation or a legal claim.

Beyond the simple mechanics of capturing mobile communications and lowering the costs of fulfilling ediscovery requests, mobile compliance solutions provide a conduit for greater insights into an organization's operations and fuel other efficiencies. Integrating artificial intelligence and machine learning into these solutions means communications can be autonomously tagged, redacted, and analyzed in near real time, providing a complete and ongoing understanding of all an organization's communications that can proactively identify potential compliance risks.

Q. What other benefits beyond GRC compliance can be derived from greater analysis of an organization's mobile and digital communications?

A. Robust mobile compliance solutions provide benefits to organizations beyond improving their risk management profile. A strong GRC reputation breeds trust with customers, who know they can rely on a company to protect their data. That trust strengthens business relationships and can drive new opportunities for customer engagement, resulting in revenue growth. Analysis of data from communications compliance systems can help identify ways to optimize an organization's overall IT and communications strategy as well as highlight best practices that can improve employee and customer engagement. Insight into usage of employee and customer communications tools can identify underutilized or redundant technologies than can be consolidated for cost and efficiency improvement.

Q. What should organizations look for in evaluating potential mobile communications compliance vendors?

A. There are three main elements to consider when evaluating mobile and digital communications compliance tools: connectivity, features, and ease of use/deployment.

- **Connectivity.** For communications compliance and management tools to work, they need to be operational wherever the employee is located. Pervasive, reliable, and secure connectivity — whether cellular, Wi-Fi, or wired — is a prerequisite. As with any communications-related tools and services, looking at the coverage and reliability of connectivity is critical. If employees are unable to engage in digital communications because they are out of range or have a bad connection, the value and benefits of compliance solutions are for naught.
- **Features.** Once that ubiquitous connectivity layer can be ensured, the next step is to evaluate the solution's feature set. In addition to recording and archiving the required communications modalities, what cataloging/tagging functionality is provided? Is there the ability to redact sensitive information prior to transfer to third parties? What are the data storage and cloud compute requirements? Are the features available in a one-size-fits-all approach, or can functionality be selected à la carte to adapt to each industry's regulatory requirements? What analytical tools and policy controls are available in the management portal? Can policies be controlled by employee rank or device type?
- **Ease of use/deployment.** Of course, the end-user experience is an integral consideration to ensure that the solution helps meet the organization's compliance needs. If a solution is difficult to use, is distracting, or creates more work for the end user, employees may look for ways to circumvent its usage, reducing the value and exposing the company to future risk. The organization also must discuss with the vendor how its mobile compliance solution integrates with the company's existing mobile device management (MDM), customer relationship management (CRM), and knowledge management investments.

It is also a good practice to ensure that the compliance solution vendor meets key industry standards and certifications, such as ISO 27001, which covers how to manage information security. These certifications ensure that the vendor is aligned with industry best practices.

Further, the organization should carefully consider a potential mobile communications compliance vendor's broader partnership ecosystem. Most compliance tools rely on multiple technologies, such as AI/ML, cloud storage, and edge compute to enable a robust, flexible solution. Any solution must be able to scale and evolve to match the organization's growth and the ever-changing regulatory landscape.

About the Analysts

Jason Leigh, *Research Manager, 5G and Mobile Services*

Jason Leigh is a Research Manager for IDC's Mobility team responsible for 5G and mobile operator research. Jason's research focuses on the strategic implications and market opportunities presented by the emerging 5G ecosystem, including commercial availability, installed base forecasts, regional adoption trends, content and services enablement, device impacts, 5G's role in the Internet of Things (IoT), and innovative use cases leveraging 5G.

Sandra Wendelken, *Senior Research Analyst, Mobile and IoT Services*

Sandra Wendelken is a Senior Research Analyst for IDC's Telecom and Mobility team focusing on mobile and Internet of Things (IoT) services. In this position, her research covers the mobile operator market in the United States and globally. Sandra provides detailed analysis on IoT connectivity services, public safety and first responder communications service offerings, managed private mobile networks, and other emerging service trends in the mobility market.

MESSAGE FROM THE SPONSOR

T-Mobile has America's largest, fastest, and most reliable 5G network, imagined for tomorrow but ready to give you an edge today. At T-Mobile for Business, we're focused on providing your business with connectivity solutions and dedicated, exceptional service you need to help you stay ahead. To learn more about how a second line solution can help you manage compliance, visit T-Mobile for Business MultiLine.

Fastest: *Based on median, overall combined 5G speeds according to analysis by Ookla® of Speedtest Intelligence® data 5G download speeds for Q2 2022.* ***Most Reliable:*** *According to independent third-party umlaut from crowdsourced user experience data including task completion (Jan to July 2022). See 5G device, coverage, & access details at T-Mobile.com.*

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2022 IDC. Reproduction without written permission is completely forbidden.