smarsh®

Managing Communications Risk:
Insurance

Insurance companies are working hard to align their oversight processes with the ongoing digital transformation of the business world. In the last year, that transformation was propelled by the pandemic — moving many professionals to home offices. The swift adoption of tools like video conferencing, collaboration platforms and mobile chat applications forever changed the way organizations communicate.

Catching up with these changes in the face of regulatory obligations, developing consumer data privacy laws, cybersecurity issues and legal risks has created several distinct challenges. Insurance companies are no strangers to managing risk. Getting in front of potential issues is a critically important calculation that requires a holistic approach to decide which new communications tools to allow your organization to use for conducting business.

Risk-averse insurance companies must give employee communications diligent examination as a major risk factor. As insurance firms pursue digital transformation strategies, they must also engage all functional stakeholders to examine various risk factors. Data leaks, intellectual property loss, regulatory violations or misconduct are harder to track when employees and clients are communicating through multiple channels. Streamlining and managing communications data can provide a powerful defense against these common business risks.

In today's digital world, a solution for preserving and monitoring communications is a necessary tool for insurance companies.

In this guide we'll cover:

- Communications recordkeeping and retention requirements for insurance companies
- Holistic risk management in an era of unlimited electronic communication
- The benefits of cloud-based communications data warehousing
- Tips for creating a risk management strategy while enabling employee communication
- How Smarsh helps insurance organizations proactively manage communications risk

Manage regulatory requirements

Insurance companies are regulated by a combination of watchdog organizations and consumer protection legislation:

National Association of Insurance Commissioners (NAIC):

Insurance companies must maintain books and records to comply with individual state record retention requirements

Financial Industry Regulatory Authority (FINRA):

For brokerage operations, FINRA 4511 requires the preservation of books and records for at least six (6) years, and FINRA 3110 requires a supervision system for associated brokers

Health Insurance Portability & Accountability Act (HIPAA):

Appropriate administrative, physical and technical safeguards must be in place to secure protected health information (PHI)

Employee Retirement Income Security Act (ERISA):

Fiduciary plan documents, contracts and agreements, participant notices and compliance documents must be retained for at least six (6) years after filing date

Dodd-Frank Act:

Brokerage firms are required to establish and maintain procedures to maintain and preserve records for a minimum of five (5) years

So, considering the growing use of video conferencing, voice recording, social media and mobile applications, what is a business record in this context? While specific language varies from state to state, the spirit of recordkeeping requirements is that the information pertains to the business, whether related to potential risk or value. Considering the explosion of digital communications, wrangling, preserving and managing that content has gotten exponentially more complicated.

In the case of a regulatory audit, security breach or legal issue, not only are communications (emails, chats, texts, etc.) to be examined. The associated metadata (time stamps, edits/deletion of data, etc.) can have a material impact on a firm's ability to sufficiently satisfy a regulatory or legal request.

At the same time, insurance organizations must be cognizant of data privacy laws such as the General Data Protection Legislation (GDPR) in the EU, the California Consumer Privacy Act (CCPA), and a variety of other U.S. state and international privacy regulations. Companies must now be more diligent than ever to ensure they're using personal information only for its stated purpose. They must have a fast and reliable means to meet Right of Access requests.

Recommended Reading:
Managing Global Data Privacy Laws and Communication Regulations in Financial Services

View risk holistically

New communications tools combined with the move from centralized offices to distributed home networks create a brand-new set of risks:

- **Cybersecurity risks:** The use of unsecured home networks and unauthorized devices creates blind spots for IT and security teams, paving the way for increases in fraudulent activity
- **Regulatory risks:** When communications tools are downloaded or deployed before policy controls can be implemented, compliance gaps exist if those communications are not being archived or monitored
- **Legal risks:** The distribution of communications across multiple tools, devices and networks can increase the risk of intellectual property loss, employee misconduct and reputational damage
- **Data privacy risks:** Privacy complications can arise if collaboration tools are not used exclusively for business purposes

Whether workers are on a mobile device, working at home or in an office, they need to be able to communicate securely and compliantly. Having a comprehensive view of those communications — and the ability to find and resolve issues efficiently and proactively — is a critical step toward ensuring that cybersecurity, regulatory, legal and data privacy risks are being managed.

This kind of agility is made possible with a modern, cloud-based solution for compliance, supervision and e-discovery.

Adopt a cloud-based, streamlined solution

Prior to the pandemic, many insurance firms were reluctant to move to cloud-based technology for managing information risk. Oftentimes companies are held back by concerns about the cost and risk of migrating data and adopting new tools. Perhaps there is institutional inertia when it comes to changing how things are done and the resources that would be required. Legacy archiving and monitoring technologies are often embedded into business processes.

But how much is supporting old systems in a new world of hybrid workforces costing these organizations?

Outdated, disparate infrastructure that was built for managing email and phone monitoring makes insurance companies vulnerable to the risks that lie hidden in today's Slack chats and text messages.

With outdated technology for managing communications, companies are likely supporting multiple systems that aren't integrated, don't scale, and cost valuable resources to manage. Plus, there are opportunity costs to maintaining stagnant technology. For example, enabling the latest conferencing tools offers a new channel for connecting with clients.

Moving to the cloud might be perceived as a risky endeavor, but it provides insurance companies with the tools to get ahead of business risks. Delaying a move toward modern technology and maintaining the status quo can inhibit business growth and cause problems down the road.

Recommended Reading:
Financial Services Move Toward a Greener, More Sustainable Future

Enable your organization

Ultimately, upgrading to modern, scalable, integrated technology for managing communications is not just about mitigation of risk. It's about enabling employees to be more effective in the way they engage with clients and each other.

The events of the past year and the uncertain future of the workplace should be a catalyst for modernizing compliance, risk management and e-discovery practices in the insurance industry. Business communications are happening through an ever-expanding network of channels (email, chat, text message, collaboration, conferencing, mobile apps, etc.) that all need to be accounted for. CCOs and risk management professionals can take this chance to explore innovative approaches and strategies to modernize and future-proof their efforts.

To stay ahead of compliance, security and legal risks, insurance companies should start with the following practices:

1. Install a cross-departmental communications governance council to collectively make decisions about communications technology and the implied risk across the business
2. Implement or update internal communications policies so employees are aware of permitted or prohibited communications channels and supervision practices
3. Deploy a cloud-based solution for collecting, preserving, monitoring and producing communications (preferably AI-enabled to pinpoint red flags and serve up business insights)

The tools people use to collaborate will continue to evolve. This makes information risk management an ongoing challenge. Lessons learned from 2020 can serve as a guide to prioritize updating policy, technology and training — and better prepare for the next wave of communications channels to emerge.

Smarsh Can Help

Smarsh can enable a smooth transition to a cloud-driven business, with improved data visibility across all communications content:

- Native content capture
- Secure books-and-records storage
- Efficient supervisory review
- Intelligent surveillance
- Reduced e-discovery risk and cost
- End-to-end data security and privacy

Representatives from cross-departmental functions in insurance can benefit from Smarsh solutions:

Compliance

Comply with NAIC and state recordkeeping requirements as the explosion of new communications sources are being used by remote staff. Smarsh provides visibility and control over all communications via capture, archiving and supervision technology.

IT

Leverage a cloud-based communications data warehouse to enhance business agility and move away from calcified, on-premises systems that limit growth. Smarsh has built our modern Enterprise Archive with cloud-native architecture to enable business growth and response to change.

Legal

Reduce the time and expense of e-discovery due to high and unpredictable costs of outside service providers, especially when the information is disparate and lacks context. Filter unneeded content and view communications in their native state. Have greater control over the e-discovery process.

Risk/InfoSec

Smarsh provides the ability to identify and respond to cyber and fraud risks. Typically, companies have limited visibility into legacy content repositories. Enterprise Archive makes content easily searchable and can help spot red flags. Its AI-powered applications can identify patterns and trends to proactively manage risks.

smarsh®

Smarsh® is the recognized global leader in electronic communications archiving solutions for regulated organizations. The Smarsh Connected Suite provides innovative capture, archiving, e-discovery, and supervision solutions across the industry's widest breadth of communication channels.

Scalable for organizations of all sizes, the Smarsh platform provides customers with compliance built on confidence. It enables them to strategically future-proof as new communication channels are adopted, and to realize more insight and value from the data in their archive. Customers strengthen their compliance and e-discovery initiatives, and benefit from the productive use of email, social media, mobile/text messaging, instant messaging and collaboration, web, and voice channels.

Smarsh serves a global client base that spans the top banks in North America and Europe, along with leading brokerage firms, insurers, and registered investment advisors. Smarsh also enables federal and state government agencies to meet their public records and e-discovery requirements. For more information, visit www.smarsh.com.

US: 1-866-762-7741 | UK: +44 (0) 20 3608 1209 www.smarsh.com @SmarshInc SmarshInc Company/Smarsh