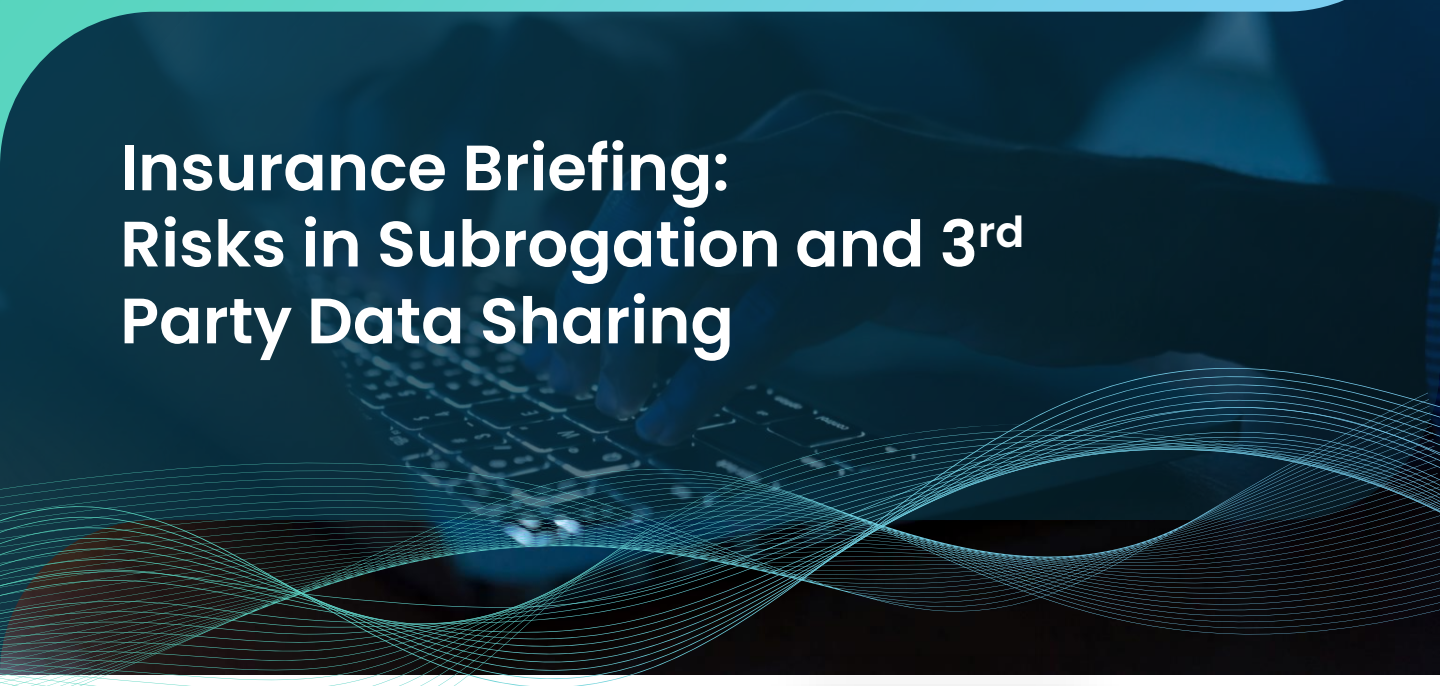
1touch.io
Data Aware Security

Insurance Briefing: Risks in Subrogation and 3rd Party Data Sharing



Today's Challenges: Sensitive Data Visibility

CISOs, Information Risk professionals, and security analysts are fighting in the dark; They may know roughly from where the invaders are coming , and can throw more resources toward the potentially vulnerable areas, but are they always protecting the right data assets?

More specifically, the world of insurance is especially at risk since so much business value is driven from analyzing and understanding PII and individual risk. Between consolidation in the insurance industry where M&A is common, to subrogation and sharing PII or PHI with third parties, risk mitigation is required...but risks remain hidden without a clear, accurate and actionable data inventory.

Highlights

- Sharing data outside the organization is risky no matter how much the third party is trusted
- Up to **30% risk reduction** through the use of sensitive data intelligence that discovers unknown datasets that require protecting
- Subrogation can be a risky action but with the right control's insurers can rest easy
- Classification accuracy at, or above **96%** leads to greater usage of sensitive data intelligence to fuel the business

Specifically, subrogation – the act of the insurer working with a third party investigation firm to evaluate if an accident was actually caused by the other party – requires the sharing of a full record including PHI, PII, and potentially business sensitive information. Typically, this sharing is done via secure file transfer tools that sit at the organization's edge and send large files full of insurance records to be investigated. However, does every piece of that record need to be shared? As a Security, risk or privacy leader in an insurance company, how can you know what data is being sent? Can you verify that ONLY relevant, business-needed data is being shared?

These are tough questions that require a strong data foundation and hygiene in order to answer. In a perfect world, there would be a single data inventory that is automatically updated so it is always current. Then, the CISO's organization would have full visibility into what specific data elements are leaving the environment with clear rules in terms of how that data is being used as well as notifications once the data officially changes hands. Similarly, there'd also be rules and validation that says that after X days, if a case is no longer active, then the data is destroyed with a receipt back to the source organization.

The key to visibility and removing risk from subrogation and third-party data sharing is to have a granular, accurate and automated inventory for all data that enables decision makers to prioritize their actions. **1touch.io Inventa™** is this single source of truth – a full scale discovery, classification and inventory for all the organization's data, with simple dashboards to visualize risk and prioritization. **1touch.io Inventa ™** becomes the source of sensitive data intelligence that can be easily shared to other solutions to create a smart, efficient data security and privacy posture that is focused on what matter most – the business-critical data.

1touch.io Inventa's ™ approach is designed to remove humans from the loop to free them to focus on other tasks.

Starting at the network layer, **1touch.io Inventa ™** begins to discover and classify sensitive data as it moves throughout the environment as a means of understanding where the sensitive data is resting. Once the network is mapped and it is clear where the data is sitting, then **1touch.io Inventa ™** deploys and scans – which are in excess of up to 96%+ accuracy, out of the box and 99%+ with minimal tuning – to start building the data inventory at both the data element and the repository level. Once the inventory is built, now **1touch.io Inventa ™** can be the dashboarding tool to prioritize risk and protection as well as using its open APIs and pre-built integrations to feed sensitive data intelligence to other mission critical tools to focus only on the data that matters the most.

1touch.io Inventa ™ helps security professionals answer four core questions:

1. What data do I have?
2. What data is sensitive?
3. Of the sensitive data, is it all protected?
4. Of the protected data, what is not sensitive and doesn't need to be protected?

Conclusion –
Reduce risk, increase visibility and sleep well at night!

As data continues to proliferate and move out to the cloud from the traditional data centric or mainframe environment, it's more and more important to have strong data visibility to ensure the right data is being protected, used, or deprecated. From the insurance industry perspective, subrogation is an established part of the business but one that can be improved due to reducing risk and sharing only what needs to be shared. Having strong sensitive data intelligence will make the entire process smarter and more context-aware leading to better decision-making and security posture.

1touch.io is here to be your partner in tackling Subrogation 3rd-party data sharing challenges, especially around the need-to-know what data is involved. As the ONLY best-of-breed, dedicated discovery and classification solution in the market, **1touch.io's Inventa ™** can provide the required level of sensitive data intelligence for any data in any repository while it's at rest and in motion across the network.

Contact us to learn more about how we can help with Subrogation or other challenges.