INSURANCE TECHNOLOGY STRATEGY AND REGULATORY COMPLIANCE, VOL. 1

AUGUST 2019

Summary

Locke Lord LLP and Novarica look at new regulatory developments in analytics, use of data, and data security that have the potential to affect insurer technology strategy.

This edition reviews the potential effects of regulation on the use of analytics and AI in life insurance underwriting, how privacy requirements may affect insurer data governance and MDM strategies, and how third-party data security requirements may affect distribution technology strategies.

Contents

Primary Report Contacts

Mitch Wein
Senior Vice President,
Novarica

Brian Casey
Co-Chair, Regulatory & Transactions
Insurance Group, Locke Lord

Page Count
10

INTRODUCTION

Novarica and Locke Lord have launched a quarterly series to help insurance leaders understand the potential implications of regulatory changes on their technology strategies.

This edition focuses on data privacy issues that have the potential to affect insurer data and analytics strategies. Increasing data volumes and the growing power of analytical tools are making it possible for insurers to target customers and manage risk more effectively than ever before, but regulators are concerned with maintaining fairness in the insurance market.

The increased flow of data between counterparties creates additional questions about responsibility for data protection throughout the entire value chain. This report looks at three issues affecting insurer technology strategies in these areas.

New York Circular Letter No. 1 and Life Insurance Underwriting

Locke Lord provides an overview of NYDFS' circular letter no. 1 and explains its impacts on the use of AI and machine learning in the life insurance space. New York State has taken the lead in implementing aggressive regulations, and other states seem likely to follow their lead. Novarica reviews the current state of analytics and life insurance underwriting and highlights key technology issues related to this circular letter.

California Consumer Privacy Act of 2018 and GBLA

Locke Lord discusses the California Consumer Privacy Act of 2018 (CCPA) and its relation to the Gramm-Leach-Bliley Act governing data sharing by financial institutions. The CCPA gives California residents the right to know what data companies have collected about them and why, to request deletion of personal data, to opt-out of sales of their personal data (identifiers, biometrics, geo-location, internet browsing history, etc.), and to access their personal information easily. Novarica highlights the implications for insurer data governance and master data management strategies.

NYDFS Cybersecurity and Third-Party Service Provider Requirements

Locke Lords reviews challenges in compliance with the third-party service provider (TPSP) requirements of the NYDFS Cybersecurity Regulation, which can be especially challenging for large covered entities with a multitude of TPSP types. Novarica discusses the potential impact for insurer distribution connectivity strategies.

Note: Throughout this report, Locke Lord's legal summaries, which do not constitute legal advice to any person, are presented at the beginning of each section in a highlighted box. Novarica's analysis and opinion is presented following the summary.

NY CIRCULAR LETTER NO. 1 AND LIFE UNDERWRITING

How do you prove that something is not discriminatory? While a simple question on its face, New York's recent Circular Letter No. 1 regarding New York licensed life insurers' use of big data has the industry spinning in circles as it attempts to understand what it means to comply with the Circular Letter's restrictions regarding their use of "unconventional sources or types of external data" in underwriting.

Specifically, life insurers are prohibited from utilizing external data sources, algorithms, and predictive models for the purposes of underwriting or rating, unless the insurer can ***independently*** establish that the processes do not:

- collect or utilize prohibited criteria; or
- result in underwriting or rating guidelines that are unfairly discriminatory.

Moreover, the Circular Letter makes clear that: "even if statistical data is interpreted to support an underwriting or rating guideline, there must still be a valid rationale or explanation supporting the differential treatment of otherwise like risks. The second part of this inquiry is particularly important where there is ***no demonstrable causal link*** between the classification and increased mortality and also where an underwriting or rating guideline has a disparate impact on protected classes." As such, it is likely that New York would frown on an algorithm based on how many times a consumer watched Beyoncé video on YouTube.

Finally, the Circular Letter also requires that the insurers must provide the specific reason or reasons for a declination, limitation, rate differential or other adverse underwriting decision, including the material elements of an accelerated or algorithmic underwriting process, and the external data sources upon which it relies.

Taken together the requirements of the Circular Letter are having an immediate chilling effect on the use of AI and machine learning in the life insurance space, as insurers are wary of violating the Circular Letter and facing fines, suspensions and revocations of product approvals.

Benjamin P. Sykes, Locke Lord LLP

Life Insurer CIOs need to consider how to handle this interpretation of the law in the context of third-party data use. This includes the following use cases covered by the Novarica New Normal 100 capabilities model.

- **Pre-Underwriting.** Using internal and third-party customer data to target based on probability risk and provide indication of premium upfront. Carriers need to document data selection criteria and must disprove statistical bias explicitly in categories like race, faith, education, occupation, and sexual orientation. 39% of life insurers who participated in the Novarica New Normal 100 benchmark in 2019 had current capabilities in pre-underwriting; 28% reported active or planned pilots.
- **Analytics-Driven Targeting.** Using analytics to identify customers with unique characteristics and tailor marketing to them. Publicly available data (e.g., social media data) can help carriers identify high-risk activities like smoking, cannabis use, and drinking. Organizations will need to analyze social media data so as not to generate wrong conclusions. 56% of life insurers report current capabilities in this area; 33% report active or planned pilots.

- **Rules-Based Offer Guidance.** Capability to guide distributors to a best-fit product by analyzing data provided or third-party data. Carriers can use AI-enhanced algorithms, but the logic needs to be transparent. CIOs should not deploy opaque models which create a black box around how data patterns and algorithms work. Each piece of a total decision must be explainable. 56% of life insurers report current capabilities in this area; 11% report active or planned pilots.
- **Pre-Fill Data.** Leveraging internal or external data sources for pre-fill of key information to streamline application submission and determine whether to waive some medical exams. As an example, CIOs can deploy automated processes that ingest third-party pharmaceutical data to avoid fluid collection as part of the submission process. CIOs can also harness the power of natural language processing (NLP) to harvest doctors' notes, reports, and various images (x-rays, CAT scans, MRI) to create usable unstructured data for the underwriting process. 78% of life insurers report current capabilities in this area; 11% report active or planned pilots.
- **Analytics-Driven Product Design.** Incorporating customer behaviors, customer value, market capacity, and other nontraditional factors and analytics into the product design. As long as this data is de-identified as part of the process the CIO designs, the product design will not be viewed as discriminatory. 67% of life insurers report current capabilities in this area; 6% report active or planned pilots.

The portals that carriers built to support agents or customers directly should contain disclaimer language that clearly informs users of what third-party data they collect and where they will use it. The portals should have clear audit logs that demonstrate how and where data is used. Portals should also have a place where policyholders or agents on behalf of policyholders can authorize the transmission and collection of electronic health records, biometric data from wearable devices, as well as behavioral and lifestyle data. Carriers should document and make auditable how they use this data in the underwriting process and in rating risks.

Different life events often motivate life insurance purchases. Carriers can collect third-party data from public sources (e.g., wedding and baby shower registries, signals on social media that indicate upcoming retirement) and use this information to generate emails, modify CSR scripts if the policyholder calls the help desk, or alert agents so they can reach out to insureds to suggest additional products.

Perhaps the greatest use of third-party data in life insurance will be to validate internal data that the organization has already collected. This avoids regulatory pitfalls. Life insurers often have multiple legacy systems, with siloed data and inaccurate data from poor historical processes and screen edits. Third-party data can verify what insurers have already collected and enable insureds to identify data that requires correction (e.g., email addresses).

CALIFORNIA CONSUMER PRIVACY ACT AND GLBA

Insurance companies and producers, banks, and other financial institutions (as well as other businesses) transacting business in California are busy preparing for the January 1, 2020 effective date of the California Consumer Privacy Act of 2018 (CCPA). *But why, given the federal Gramm-Leach-Bliley Act (GLBA) exemption of the CCPA?* Unfortunately, the CCPA's GLBA exemption is not comprehensive, and presents compliance challenges to financial institutions covered by the GLBA.

Basically, the CCPA (as amended by SB 1121) provides that the CCPA does not apply to information collected, processed, sold or disclosed under the protections of the GLBA and its implementing regulations. Unfortunately, the CCPA applies to "personal information," which is defined much more broadly than "nonpublic personal information" as defined by the GLBA. Therefore, financial institutions must apply the CCPA's requirements to the data they collect, process, sell or disclose that meets the CCPA's very broad definition of "personal information" but is not GLBA "nonpublic personal information." Examples include IP addresses and tracking information collected through a website, and geolocation data.

It is also important to note that the CCPA provides a similar exemption for medical information and protected health information collected under the federal health laws HIPAA and HITECH, and related regulations. This HIPAA exemption, however, can be expanded by health care providers to the extent that the health care provider voluntarily treats other patient information "in the same manner." This option, not available under the GLBA exemption, would appear to undermine any potential argument that a financial institution could voluntarily treat information other than GLBA nonpublic personal information in the same manner, and claim it too is exempt from the CCPA's requirements.

Finally, the GLBA exemption does not apply to a consumer's private right of action under the CCPA in the event a financial institution experiences a data breach involving his or her personal information. Therefore, in the event of a data breach, a consumer could sue the financial institution for statutory damages by claiming a violation of the CCPA's requirement to provide "reasonable security," even if the information at issue was subject to the GLBA and protected as required by the GLBA's Safeguards Rule.

Ted Augustinos, Locke Lord LLP

A CIO will need to deploy various forms of automation to comply with the CA Consumer Privacy Act. This includes systems that:

- Deploy consent management tracking, including expiration
- Manage service providers for compliance with Do Not Sell and Right to be Forgotten requests
- Provide audit trails for customer data interactions for data correction and fulfillment of personal data requests

There are a number of packages a CIO can use to achieve these capabilities, including Big ID, Citrix, IRI, Metric Stream, OneTrust, Oracle, Qualys, SAI, SAP, SAS, and Veritas.

A CIO should also work closely with the chief compliance officer and legal staff to design the supporting processes necessary for compliance. Guidance around proper governance, information risk management, and third-party risk management will be key to avoiding fines.

A foundation to the entire program will be a data dictionary and thesaurus (sometimes called a metadata repository). These identify where the data is, its synonyms across the data processing ecosystem, categories of each piece of data, and rules around data categorizations. The dictionary will also allow the CIO and data team to see data lineage, which will allow them to understand the various stages of data transformation and the data's source. The data dictionary can store whether the data is "nonpublic personal information" or just "personal information," depending on the context.

The CIO's data team will need to understand specific operational details around customer data, including answers to questions like:

- Can you get a 360-degree view of a client?
- Is there an issue with duplicate customer data?
- Any issues with agent/policyholder authentication for portal access?
- Any issues with accuracy of provider specialty?
- Any issues with accuracy of provider roster for large institution?
- Any issue with customer contact information such as address, phone, and email?
- Does doctor claims experience follow clients if they change institution?
- What data challenges occur when a medical practice is acquired by a larger institution?

IT data questions will also need answers to comply fully with the regulations. These include:

- What is the archival policy for structured data? Content (emails, documents)?
- How many times is data replicated? Production, disaster recovery, development, testing, user acceptance testing, etc.?
- How is access to sensitive data controlled?
- How is sensitive data identified/located?
- How is test data created?
- What is the process for "legal hold"?

The CIO needs to work with the CISO, chief data officer (CDO), and data architects to determine if different systems represent key master data differently or if a master data repository exists in an MDM infrastructure which has resolved these differences in one location. The MDM repository should hold rules about what data requires encryption at rest and in-transit as well as in which states this is applicable. Security regulations require organizations to understand where and how they use data. Personally-identifiable information (PII) and healthcare data are of particular importance, as is knowledge of where data exists, what its permitted uses are, ownership in the carrier organization, and access control.

NYDFS CYBERSECURITY & 3RD PARTY SERVICE PROVIDERS

Among the various obligations imposed on "covered entities" under the NYDFS Cybersecurity Regulation (NYCCR 500), which became fully effective in March 2019, is the duty to address potential cybersecurity events that may arise from business relationships with "third party service providers". A third-party service provider ("TPSP") is any person other than an affiliate that provides services to a covered entity and, through its provision of those services, maintains, processes or has access to "nonpublic information" of a covered entity but excludes affiliates of the covered entity. Compliance with the TPSP requirements of the NYDFS Cybersecurity Regulation can be one of the most onerous of its obligations, especially for large covered entities that have a multitude and wide range of different types of TPSPs.

Covered entities must adopt and implement written policies and procedures designed to ensure the security of their information systems and nonpublic information to which their TPSPs have access or nonpublic information that their TPSPs hold. These policies and procedures must be based upon the risk assessment required to be conducted by a covered entity, and at minimum must include:

- identification and risk assessment of each TPSP;
- minimum cybersecurity practices that TPSPs must satisfy;
- due diligence processes used by the covered entity to evaluate the adequacy of a TPSP's cybersecurity practices; and
- periodic assessments of TPSPs conducted by the covered entity based on the risk they present to the covered entity and the continued adequacy of their respective cybersecurity practices

In addition, a covered entity's TPSP policy and procedures must address:

- TPSPs' own policies and procedures for information systems access control, including their use of multi-factor user authentication;
- TPSPs' use of encryption for both data at rest an in transit;
- requiring TPSPs to notify the covered entity if a TPSP experiences a cybersecurity event that impacts the covered entity's information systems or nonpublic information; and
- required representations and warranties from TPSPs to the covered entity procedures relating to the security of the covered entity's information systems or nonpublic information.

Insurance companies have wrestled with the definition and requirements of TPSP as it applies to their relationships with producers. Many questioned whether appointed insurance producers are TPSPs of an insurance company, and if so, whether the difference between a captive or independent agency distribution force matters. The NYDFS declined to except producers from the definition of TPSP, taking the position is that appointed insurance producers may be TPSPs of an insurance company, even though an appointed producer licensed by the NYDFS is also a covered entity in its own right. In fact, some producer agreements expressly articulate that the producer is, under the agreement, rendering services to the insurance company. Conversely, the insurance company may be a TPSP of a producer, and each may be the TPSP of the other.

Brian Casey, Locke Lord LLP

CIOs and CISOs jointly will need to establish an attestation program for third parties their carrier does business with, including:

- TPA
- Vendor
- Agency/Broker
- BPO Provider
- Outsourcer
- Reinsurer

The attestation should require the third party to attest that it complies fully with the New York State cyber regulations, document where it does not comply, and specify a timeline with high-level action steps for remediation.

Contracts will require revision to ensure that the carrier/CIO/CISO has the right to perform periodic security audits of the third party to verify its compliance and in the event that a carrier suspects a security issue or an inaccurate attestation for whatever reason.

The third party needs to pay fines that the carrier may incur if data becomes exposed. Carriers should have strong indemnity protection in their contracts with third-party service providers and should require them to maintain a minimum amount of errors and omissions and cyber insurance coverages.

The CIO and CISO should arrange to have firms available to perform security audits on their behalf if needed. They also need to identify firms that can perform computer forensics investigations and maintain a chain of custody in the event a carrier's data is stolen from a third party.

CIOs and CISOs should perform event simulations which include representatives of third-party organizations. A simulation of a malware event that steals data through the firewall, for example, should have a scenario that includes the firewalls of the carrier's outsourcing firms.

How a CIO and CISO ensure their agents are compliant with the NY State regulations is of particular interest here. This may be easier of the agent is captive and uses the carrier's infrastructure and systems. However, independent agents will use their own infrastructure, have their own networks, and utilize their own AMS software (e.g., Vertafore, Applied) as well as supporting spreadsheets.

Some CIOs are providing security audit services to these agents. Others are working with their distribution executives to change distribution agreements to mandate multi-factor authentication, data encryption at rest and in-transit, and audit log proof that they treat non-public personally identifiable information (PII) confidentially. Some wholesale brokers require attestations from the carriers. CIOs must ensure in those cases that the processes around multi-factor authentication and encryption are documented and that the tools enforcing these processes create logs that are easy to audit.

It is possible for CIOs in global insurers that data is being shared across affiliated or subsidiary countries, sometimes across international borders. Attestation and audit processes may still be required between subsidiaries of the same holding company in these cases.

Organizations can reuse processes and technologies they put in for New York state as the basis for compliance with other state data security regulations, like those in Alabama, California, Connecticut, Michigan, Ohio, South Carolina, etc.

CONCLUDING THOUGHTS

The bottom line is that data use and security regulations will keep evolving. Regulations and underlying definitions may be different or in conflict with each other. CIOs and CISOs will need to work with their legal advisors to understand existing regulations and new regulations as they emerge, assess the processes and technology deployed, and determine if and how to reuse processes and technology. It will be important for insurers to bring in advisors to provide specific expertise where needed and to raise awareness of these issues with all third party business partners.

Related Research

- Key Issues in Preparing for NY State Cybersecurity Regulations
- IT Security Update 2019
- Novarica New Normal for Life Insurers 2019
- Master Data Management in a Big Data World
- Emerging Technology in Insurance: AI, Big Data, Chatbots, IoT, RPA, and More

ABOUT NOVARICA

Novarica helps more than 100 insurers make better decisions about technology projects and strategy. Our research covers trends, best practices, and vendors, leveraging relationships with more than 300 insurer CIO members of our Research Council. Our advisory services provide on-demand phone and email consultations on any topic for a fixed annual fee. Our consulting services include vendor selection, benchmarking, project assurance, and IT strategy development, providing rapid, actionable insights and guidance, delivered directly by our senior team. www.novarica.com

ABOUT LOCKE LORD LLP

Locke Lord is a full-service law firm with global reach and 20 offices designed to meet clients' needs in the United States and around the world. The Firm has a history that spans more than 130 years and is a leader in the middle market arena. Locke Lord focuses on providing the highest levels of commitment, quality and service to clients across its five Key Sectors: Energy and Infrastructure; Finance and Financial Services; Insurance and Reinsurance; Pharmaceutical; and Private Equity. In addition, the Firm advises clients across a broad spectrum of other industries, including fund formation, venture capital, health care, public finance, real estate, technology, cybersecurity and white collar, while providing a wealth of experience through its complex litigation, intellectual property, tax, regulatory and transactional teams. www.lockelord.com

Authors

Mitch Wein is a Senior Vice President of Research and Consulting at Novarica. He is an expert in international IT leadership and transformation as well as technology strategy for life, annuities, health, personal and commercial lines, wealth management, and banking. Prior to joining Novarica, Mitch served in senior technology management positions at AXA in UK and Ireland, and CTO of AXA Equitable; Mitch was also CTO for the Domestic Brokerage Group and Domestic Personal Lines at AIG and held roles at Prudential Insurance. Mitch holds both an MBA in Information Systems and a BS in Finance from Fordham University.

Brian T. Casey. Brian Casey, partner at Locke Lord LLP, serves as Co-Leader of the Regulatory and Transactional Insurance Practice Group, and is a member of the Firm's Corporate, Capital Markets and Health Care Practice Groups. Brian focuses on mergers and acquisitions, corporate and structured finance and other transactional and regulatory matters for clients in the insurance, financial services and health care industries. His clients include insurance companies, insurance holding companies, insurtech start-ups, managing general agents and insurance agencies, third party and claims administrators, banks and other financial institutions, investment banks and reinsurers.

Benjamin P. Sykes is a Partner in Locke Lord's Insurance Regulatory and Transactional practice group, specializing in complex M&A, reinsurance, licensure and formation matters across the life, health and P&C lines. Ben consistently counsels InsurTechs on issues ranging from formation and product design to ongoing regulatory compliance and is a frequent speaker on the issues directly impacting innovation in the insurance industry.

Theodore P. Augustinos. co-leads the Privacy & Cybersecurity Practice Group at Locke Lord LLP. Ted leads the Group's Initiatives focused on the California Consumer Privacy Act and the New York DFS Cybersecurity Regulation, and its Incident Response Team. He is a Certified Information Privacy Professional, accredited by the International Association of Privacy Professionals. Ted serves as Co-Chair of the World Law Group's Data Protection and Privacy Group, and as Managing Partner of the Hartford, Connecticut office of Locke Lord LLP. Ted is a frequent speaker and writer on privacy and cybersecurity matters, and a guest lecturer at the Boston College Master's Program on Cybersecurity Policy and Governance.