Insight Brief

Is Your Approach to Data Privacy Reactive or Proactive?

A framework for insurers

MEYSAM SAFARI, Senior Data Scientist, IQVIA Privacy Analytics

Executive summary

Healthcare data has emerged as an invaluable resource in every organization's quest to improve engagement and drive growth. Retaining the right to use this sensitive resource demands diligent stewardship across all stakeholders and business leaders. Even one company or data supplier experiencing a privacy failure can lead to a reverse halo effect that decreases willingness to share sensitive individual data and, ultimately, stifles innovation, reduces trust, and impedes progress.

With such high stakes, data privacy is now a C-suite issue. Yet many organizations still take a reactive approach — evaluating privacy concerns as projects arise and often relying on highly manual business processes to do so. That approach is inefficient and expensive.

When organizations have a narrow view of privacy, they must slow down to rethink their strategy when presented with opportunities to leverage new sources of data, technologies, and methodologies.

A better alternative is to build a privacy strategy and implement standardized processes and systems. By operationalizing privacy in this way, business units and geographic regions within an organization can work with greater confidence, speed, and efficiency — while also delivering appropriate use and protection of sensitive healthcare data across multiple programs and initiatives. A comprehensive, enterprise-wide privacy strategy offers benefits to all stakeholders — and is well within reach for any organization committed to strong stewardship of personal data.

Introduction

Imagine if every time you wanted to drive your car, you had to inspect and reinstall the seatbelts, airbags, and other equipment that helps you travel safely from Point A to Point B. You would likely feel frustrated by the delay and inconvenience. And while you might feel comfortable taking brief rides on familiar roads, preparing the car to drive at a high speed, via a new route, or for an extended distance could be arduous and potentially risky. When it comes to data, your organization may be having an analogous experience.

You're counting on data as a vehicle for reaching an ambitious destination: better insights to drive more informed decisions. Yet you may have discovered that your organization's approach to privacy — a critical component of the safety system for data — is outdated, inflexible, and/or inadequate to forge new routes and reach the desired destinations. You're handling privacy on a case-by-case basis — implementing privacy as a tactic for specific projects, such as data linkage. What you lack is an agile and adaptive approach you can rely on for the long haul.

Automotive manufacturers have integrated sophisticated safety systems into their vehicles. Every entity looking to utilize their sensitive data has an opportunity: to develop a proactive and strategic approach to privacy. Having an effective data privacy strategy enables your organization to both protect the end consumer's data and your company's reputation while improving productivity, enabling innovation at scale, and ultimately, gaining a competitive advantage.

If data is a vehicle for navigating challenges and arriving at outcomes, then privacy strategy is a critical component of the safety system that protects the people represented in the data — and enables speed, agility, and efficiency.

Reactive privacy measures are unsustainable

There are numerous reasons why privacy is managed as a series of individual check-the-box exercises.

Perhaps there's a lack of in-depth awareness and privacy is relegated to the realm of legal and compliance teams. Perhaps privacy is viewed as a point of friction that slows achievement of engagement and business goals. Or perhaps there is recognition that privacy is important — but a lack of internal resources and expertise to tackle it more strategically.

There are even more reasons why this approach is unsustainable.

Managing privacy as a tactical, reactive exercise can leave an organization exposed as fast-changing technology fuels new threat vectors and mechanisms. Check-the-box privacy also leaves teams flatfooted in the face of even minuscule changes to project requirements. Privacy reviews that focus on only one leg of an organization's journey to outcomes miss the holistic view of how data is being used across functions and teams. So as soon as there's a chance to bring in new data, technologies, or methodologies — or to use existing resources in a new way — it forces a rethink of the entire data strategy to achieve compliance and usability. That costs precious time, budget, and focus.

Build a better 'safety system' for data

Automotive engineers have found ways to incorporate safety seamlessly into every vehicle's blueprint. In addition to installing seatbelts and airbags, they now incorporate a host of electronic sensors and alerts that don't just reduce injury from an accident; they prevent one from happening in the first place. With a privacy strategy, an organization can adopt a similar approach to safeguarding data and make the shift from reactive to proactive.

A privacy strategy is a systematic approach that addresses existing data needs and builds a foundation for managing future expansions with greater speed and cost efficiency. Privacy is no longer bolted on every time an analytics initiative is launched. Instead, it's integrated into operations, so an organization can anticipate and accommodate changes in data sources, use cases, and/or audiences. In other words, the data "vehicle" is primed to handle a variety of challenging journeys.

To drive efficiency across teams and use cases, there are core steps to reduce ambiguity, set expectations on time/cost of new initiatives, and document data holdings.

Three core steps to driving efficiency across teams and use cases

1. Start with a comprehensive review

- Assess the impact of current processes, capabilities, and resources.
- Use the assessment as baseline of privacy, current shortcomings, and the long-term benefits.

2. Evaluate the data inventory

- Perform a privacy review of existing data holdings.
- Map currently covered use cases.
- Build a roadmap for future innovation.
- Identify gaps to address from inventory of assets against future state.

3. Develop a scalable governance review system

- Establish a system to manage the volume and variety of requests from multiple business units.
- Coordinate across teams to eliminate parallel work and streamline responses to new requests.
- Provide visibility into leadership on activities and trends to improve communication and buy-in.

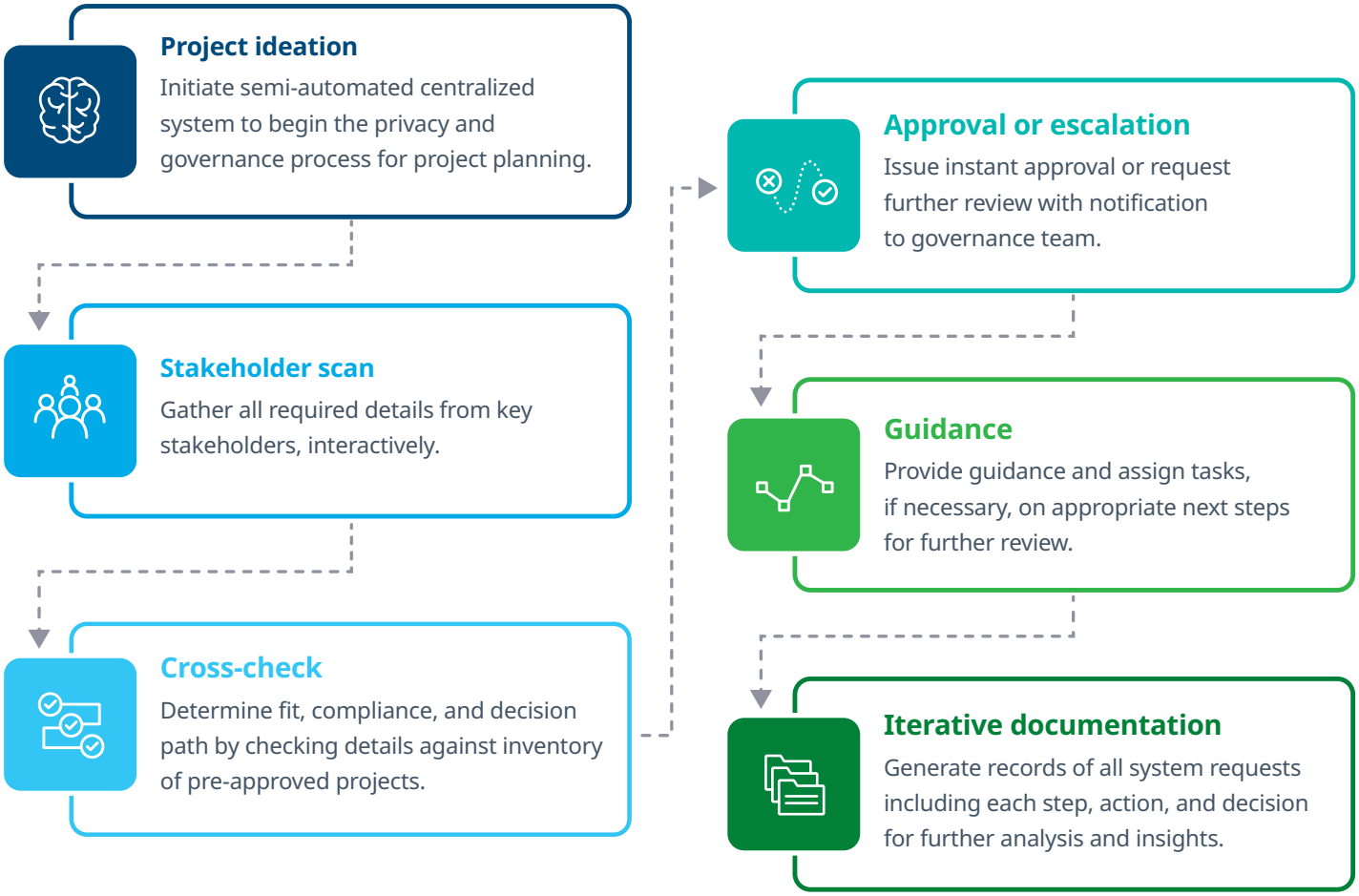
Build a better roadmap

We started with a hypothetical scenario about a car that requires drivers to install and inspect safety every time they want to take a drive. We want to end by painting a picture of a not-so-hypothetical scenario: the experience of having a well-tuned privacy strategy.

Imagine a typical company with multiple organizational functons that use data to support analytics use cases. Each team has slightly different objectives and mandates, though there may be overlap on the analytical approach or underlying data. These teams may also operate under different compliance policies when accessing datasets and performing analyses.

Having invested in a privacy strategy and supporting infrastructure, managing those differences has become much quicker and more efficient as illustrated below. The advantages of a well-automated privacy strategy and safety system are similar. The ability to initiate or modify analytics projects with greater speed, agility, and confidence results in less disruption for the project owners and a smoother ride for the organization.

A semi-automated system with clear direction and high compliance confidence



Drive toward outcomes

A privacy strategy empowers an organization to safely maximize the utility and value of data — while minimizing the cost and time of the compliance review process. It supercharges the ability to optimize and enhance artificial intelligence and machine learning (AI/ML) or actuarial models using wider range of data, identify individualized populations for outreach, design targeted initiatives, assess business outcomes with precision, and, ultimately, drive efficiencies and growth. It positions an organization to reach the most important endpoint: enterprise-wide compliant data and analytics to drive more informed consumer engagement.

To safely innovate with sensitive consumer and healthcare data, take the following six questions back to your team to evolve your privacy strategy

1. Do we have an effective approach for linking new sources of data to enhance the understanding of consumers?
2. Do we have a framework that helps us identify and evolve emerging use cases for the data?
3. Are we taking advantage of a wide array of data modalities (such as text or DICOM/image)?
4. What is our readiness for addressing new and emerging laws and standards for privacy and AI?
5. How are we governing and managing the use of AI across the organization?
6. How are we managing the broad array of regulations, including state laws, Federal Trade Commission regulations vs. the Health Insurance Portability and Accountability Act (HIPAA), and AI regulations?

Answering these questions will take you and your team to the next level in your privacy and data strategies. Refer to these questions often, as they require iterative thought as the opportunities to use data, regulations, and especially as AI continues to evolve. Carefully consider partnerships with data and privacy companies based on their capabilities and ability to respond to these points. **Contact us for more information**.

CUSTOMER NEEDS	BENEFITS OF IQVIA'S PRIVACY ANALYTICS
A reinsurance company wanted to enhance their AI/ML models by utilizing deeper, broader, and larger linked datasets from more sources including medical, mortality, and socioeconomic data in a compliant way.	Enabled linkage of various national de-identified datasets for training AI/ML models to generate faster, deeper insights.
A multinational insurance company sought to design and deploy an effective, data-driven global campaign that could adapt to local circumstances.	Marketing analysts delivered personalized campaigns at scale creating a model for improved productivity and innovation across the organization.
An insurance company with a range of products and use cases wanted to seamlessly utilize in-house identifiable datasets for secondary purposes while maintaining data compliance.	A comprehensive privacy strategy for the entirety of data holdings. A proactive look to future expansion across products and organizational functions helped resolve data blockage due to non-compliance while enabling more comprehensive business insights.
An insurance company sought to commercialize their data to drive revenue by selling data licenses to interested third parties.	A privacy strategy that encompasses data de-identification, as well as guidance on contractual requirements, and technical best practices helped the customer to commercialize their data in a privacy compliant way.

About the author

MEYSAM SAFARI

Senior Data Scientist, IQVIA Privacy Analytics

Meysam Safari is a Senior Data Scientist lead with IQVIA's Privacy Analytics. With more than seven years of experience in the privacy field, he works with companies to maximize their utilization of data without compromising privacy. He and his team conduct both big-picture analyses to identify and shape data vision and overcome gaps with respect to privacy, as well as more granular data modeling and analysis on complex linked datasets. Meysam holds a PhD in Finance from Universiti Putra Malaysia and has more than 20 years of experience in various analytical and consulting roles.

About Privacy Analytics

IQVIA's Privacy Analytics business unit delivers proven technology and expertise to enable timely, usable data that can be safely linked and put to work — in compliance with global regulations — and backed by auditable proof. More than 20 global regulatory standards (including ISO De-Identification) have been informed by our privacy experts.

CONTACT US
iqvia.com/contact