PT EN

STRATEGIC EBOOK · EXECUTIVE LEVEL

FOR CEOS, CFOS, CROS, CUOS, HEADS OF UNDERWRITING AND BOARD MEMBERS OF THE LARGEST LIFE, HEALTH, AUTO, HOME AND PROPERTY INSURERS

The Risk That Is *Priced Without Being Seen*.

How Fully Homomorphic Encryption enables insurers to price risk, fight fraud and build telematics — without ever decrypting what belongs to the policyholder.

VOLUME I · EDITION 2026 · CONFIDENTIAL

TABLE OF CONTENTS

PT EN

What you will *read*.

Appendices

PT EN

PT EN

The argument in *one* page.

If you read only one thing from this eBook, read this.

The insurance industry is, perhaps, the oldest industry in the world to operate exclusively on data. From Lloyd's in the 17th century to modern actuarial practice, all insurance exists because it is possible to price risk from collective data applied to individual cases. This logic is as old as the category. What has changed in the last twenty years is that the volume and granularity of available data exploded — wearables, telematics, clinical data, social scoring, behavioral patterns — and the industry began to depend on this new data structurally.

This dependency has created a new problem. All modern actuarial pricing depends on sensitive personal data. All modern fraud detection depends on cross-referencing sources. All personalized policyholder experience depends on a detailed profile. Each of these capabilities is necessary to survive competitively. And each, under the regulation that is coming, is a growing liability.

1

BLIND UNDERWRITING

Advanced actuarial models need clinical, financial and behavioral data — which regulation makes difficult to use.

2

STRUCTURAL FRAUD

Claims fraud costs 10–15% of total payouts. Fighting it requires cooperation between insurers — today impossible.

3

TELEMATICS STUCK

Pay-as-you-drive depends on movement data that many policyholders resist handing over.

4

OPAQUE REINSURANCE

Ceding risk to a reinsurer requires sharing data that neither side wants to expose.

FHE — Fully Homomorphic Encryption — unlocks all of these cases. It enables underwriting over encrypted clinical data. It enables collaborative fraud fighting among competing insurers. It enables telematics that do not invade. It enables reinsurance with preserved privacy.

> *"The next decade of the insurance market will be defined by which insurers manage to price risk more precisely and fight fraud in consortium — without violating the policyholder's privacy."*

THE DECISION

The question for the board is not "whether" to invest in defensible data architecture. It is how much it costs to wait until regulation, the policyholder, and the loss ratio decide for you.

CHAPTER I

PT EN

The *Risk* Industry.

Insurance is the oldest industry to depend exclusively on data. Today it is also one of the most fragile in its architecture for protecting that data.

In 2005, a life insurer priced a policy based on age, sex, profession, declared habits (smoker/non-smoker), and perhaps a simple medical test. That was it. Actuaries worked with mortality tables, sector adjustments, historical loss ratios. Data was scarce and decisions were conservative by necessity.

In 2025, the same insurer offers a policy adjusted by a health wearable, integration with an exercise app, clinical data from periodic tests, dietary-habit scoring, and possibly even polygenic genomic risk data. Each of these data points is legally sensitive, frequently a special category, and always the subject of growing regulatory debate. The modern actuary works with more data than ever — and simultaneously under more restrictions than ever.

The paradox of insurance data

Insurance is the only industry where pricing earlier, with more data, and with more precision is simultaneously the central business objective and the biggest source of regulatory risk. Every actuarial improvement is, on the other side, a new layer of exposure.

The invisible assets of an insurer

PT EN

ASSET	WHAT IT IS	WHY IT IS UNIQUE
Claims history	Years of events covered per portfolio	Only actor with complete temporal view by line of business
Fraud patterns	Identified suspicious claims	Visible in isolation, more valuable in consortium
Wearable and telematics data	Real-time behavior of the policyholder	Granularity no other industry captures
Actuarial scoring	Proprietary pricing models	Central IP of the insurer
Clinical data from health/life insurance	Exams, declarations, treatments	Special category with maximum restriction

What Changed in the Value Chain

Insurance has always been a data industry. What has changed is that five new operations have been layered on top of classical actuarial practice:

- **Algorithmic underwriting** — predictive models over granular policyholder data
- **Telematics and UBI** — usage-based insurance, especially in auto
- **Wellness programs** — discounts for healthy habits validated by wearables
- **Digital claims** — photo-based opening, chatbot, AI validation
- **Algorithmic reinsurance** — risk cession under a predictive model

THE SILENT PROBLEM

PT EN

Each of these operations depends on extensive processing of sensitive personal data, mediated by a chain of technology vendors. The Brazilian Insurance Regulator (SUSEP) and the Brazilian Data Protection Authority (ANPD) have not yet enforced intensively — but they will. And when they do, several current practices will be considered problematic.

> *"The question for the insurer's board is not whether the current data architecture is sustainable. It is how long until the first public decision reshapes the sector."*

CHAPTER II

PT EN

The Regulatory *Siege*.

Insurers live under LGPD, the Brazilian Insurance Regulator (SUSEP), and solvency regimes. All three are tightening.

LGPD and the special category

Health data is a special category under LGPD. Life and health insurance treat data of this category as raw material. Article 11 requires a specific and robust legal basis. The exceptions for "health protection" do not cover full commercial flows. In 2025, the Brazilian Data Protection Authority (ANPD) began signaling specific enforcement on the use of clinical data in insurance.

The Brazilian Insurance Regulator (SUSEP) and the traditional tension

The Brazilian Insurance Regulator (SUSEP) regulates pricing, solvency and market conduct. It wants actuarial transparency and consumer protection. Increasingly, it demands justification for predictive models — especially when they lead to refusal or premium increases. Combined with LGPD, the tension appears: SUSEP wants to know why the model decided, LGPD wants minimization of the data used.

Solvency II and the Brazilian equivalent

Solvency regimes require risk models to be auditable by the regulator. Traditional auditing requires access to data. Under FHE, it is possible to audit the model without exposing individual data.

GDPR and the European AI Act

For insurers with European operations, the AI Act classifies life and health insurance systems as high-risk. Compliance costs are high. FHE offers a path to satisfy the requirements without compromising

the competitive model.

PT EN

BIPA and US class actions

American insurers that use facial recognition in onboarding face BIPA class actions. Multi-million-dollar fines.

The conceptual turn

> *"Policy is not enough. Mathematical proof is required that data was not used improperly."*

FHE is the only technology that offers such proof. An insurer that processes data under FHE can demonstrate to the Brazilian Insurance Regulator (SUSEP), to the Brazilian Data Protection Authority (ANPD), to the policyholder and to the health partner that individual data was never accessible.

The cost of inaction

PT EN

RISK	PROBABILITY 5 YEARS	IMPACT
LGPD fine for using sensitive data without legal basis	High	2% of revenue or USD 50M+
SUSEP sanction for poorly documented risk model	Medium	Operational restriction
Class action for discriminatory premium increases	Medium	Hundreds of millions
AI Act block in Europe	High in the EU	Loss of regional market
Reputational crisis after a breach	Medium	12–24 months of renewal decline

CHAPTER III

PT EN

FHE in Executive *Language*.

No mathematics.

A transparent vault. You see that something is inside, you do not see what it is. You manipulate the contents from outside — add, multiply, compare, run entire actuarial models — without ever opening it. You return it sealed. Only the key holder opens it. This is FHE.

How it works

> ANALOGY FOR THE INSURER
>
> The policyholder encrypts their clinical or behavioral data on their own phone. They send it to the insurer. The actuarial model runs over the ciphertext and returns the calculated premium. The insurer has never seen the individual data — only the pricing result. A SUSEP audit inspects the model, not the data.

FHE vs alternatives

PT EN

TECHNOLOGY	PROMISES	FAILS
De-identification	"We removed identifiers"	Trivial re-identification
TEE	"The chip isolates"	Trusts the manufacturer
Federated Learning	"Data stays local"	Gradients leak
Differential Privacy	"We added noise"	Inadequate for individual pricing
FHE	**"Server never sees in plaintext"**	**High computational cost — but decreasing**

Use Cases by *Line of Business*.

Algorithmic underwriting over encrypted data

Modern actuarial models depend on granular data (clinical, behavioral, financial, social). Today this requires the insurer to see data in plaintext to price. Under FHE, the policyholder provides already-encrypted data, the model runs over the ciphertext, and the premium is calculated and returned. **The insurer has never seen the individual data** — only the mathematical result of the pricing.

This simultaneously solves three problems: policyholder privacy, LGPD compliance, and — surprisingly — **it increases the truthfulness of the data provided**. Several studies show that policyholders underreport conditions when they know the insurer will see them. Under FHE, the tendency is to declare more accurately because privacy is mathematically guaranteed.

Collaborative fraud fighting between insurers

Claims fraud costs between 10–15% of the total paid — billions annually. Fighting it is structurally ineffective because it requires cooperation between competing insurers: identifying fraudsters operating across multiple insurers, workshops with suspicious patterns, compromised medical experts. Today impossible.

Under FHE with PSI: insurers encrypt lists of tax IDs, IPs, workshops and physicians, discover **only the intersection**. Without revealing databases. **This is the case where FHE unlocks massive sector-wide economics that today does not exist.**

Telematics and UBI without intrusion

Pay-as-you-drive (UBI — Usage Based Insurance) is the frontier of auto insurance. But adoption is limited because many policyholders resist handing over continuous movement data. Under FHE, movement data is encrypted on the vehicle device, processed by the scoring model over the ciphertext,

and the adjusted premium is returned. **The insurer never knows where the policyholder drove** — only the aggregated score.

This unlocks UBI for segments that resist today (corporate, premium, privacy-conscious policyholders), significantly expanding the market.

Wellness program without a medical profile

Discount programs for healthy habits (steps, exercise, sleep) depend on wearable data. Today this means the insurer sees continuous health data from the policyholder. Under FHE, the data is encrypted on the phone, processed over the ciphertext, and the discount is generated without the insurer seeing any individual point. Adoption soars because the privacy barrier is removed.

Reinsurance with portfolio protection

Ceding risk to a reinsurer requires sharing portfolio data. The ceding company wants to hand over the minimum necessary; the reinsurer wants to see the maximum to price well. Constant tension. Under FHE, the reinsurer can run analysis over an encrypted portfolio — calculating exposure, catastrophe modeling, scoring — without the ceding company exposing nominal data. **Reinsurance becomes more efficient without compromising privacy.**

Digital claims under mathematical guarantee

Claim opening by photo, AI validation, digital expert review. This entire chain involves personal data. The correct pattern is the same one already consolidated in medical image diagnosis: a vision CNN (ResNet, EfficientNet) runs locally on the policyholder's app over the plaintext photo and produces only an *embedding* of a few hundred dimensions. Only the embedding is encrypted and sent. The insurer's final linear classifier (fraud/legitimate, value estimation) runs over the encrypted embedding. The insurer never sees the photo — only the encrypted verdict. A deep neural network under pure FHE is still unfeasible; a linear classifier over an encrypted embedding is already a production routine. Useful in auto (damage photos), home (property photos) and health (medical reports).

Actuarial analysis crossed with external data

PT EN

Actuaries want to cross-reference with hospital, pharmacy, and bank data. Each cross-reference is legally complex. Under FHE, cross-references can happen without either party exposing its database.

Post-quantum migration

Like banks, insurers also face the PQC transition. Adopting FHE brings, as a by-product, the technical maturity for migration — because the mathematical foundation (RLWE) is the same.

Proprietary model without training on a foreign server

Advanced actuarial models need compute power that many insurers do not have in-house. Foreign cloud is the option. Under FHE, the insurer can train a proprietary model in the cloud without exposing policyholder data to the vendor.

Compliance and private audit

Internal, external and regulatory audits require access to sensitive data. Under FHE, an auditor can validate compliance over encrypted data.

CHAPTER V

PT EN

The Economics of the *Insurer That Does Not See*.

Initial capex

COMPONENT	INVESTMENT
Founding team (crypto + ML + actuarial + legal)	USD 5M – 8M / year
Licenses	USD 300k – 1.2M
Compute infrastructure	USD 2M – 5M
Strategic consulting	USD 1M – 2.5M
Regulatory study	USD 500k – 1.2M
Integration with core systems	USD 2M – 5M
Total year 1	**USD 11M – 23M**

Annual opex

PT EN

ITEM	ESTIMATE
Compute	USD 2.5M – 6M
Maintenance team	USD 4M – 7M
Audit	USD 600k – 1.5M
Stabilized annual opex	**USD 7.1M – 14.5M**

For a Brazilian top-10 insurer with premiums above USD 5B, this represents between **0.15% and 0.3% of revenue**.

The return — six vectors

1. Collaborative fraud fighting

Estimated fraud: 10–15% of claims. For an insurer with USD 5B in claims: USD 500–750M of annual exposure. Capture via inter-insurer PSI: **USD 100–300M per year**.

2. More accurate underwriting

Access to clinical/behavioral data under FHE improves pricing by 5–15%. For a top-10 insurer: **USD 80–300M per year in loss ratio reduction**.

3. UBI/wellness with 5× adoption

Current adoption of telematics and wellness is limited by privacy resistance. Under FHE it can multiply by 3–5×. Incremental revenue: **USD 50–200M per year**.

4. More efficient reinsurance

Optimized cession with private data: **USD 30–100M per year**.

PT EN

5. Reduced regulatory risk

Hedge: **USD 20–80M of insurance value**.

6. PQC migration without rework

A by-product.

Business case

~USD 17M YEAR 1 INVESTMENT	~USD 11M STABILIZED ANNUAL OPEX
USD 800M+ VALUE ENABLED IN 5 YEARS	40×–80× EXPECTED ROI IN 5 YEARS

PT EN

“For any top-10 insurer, FHE is the digital transformation investment with the highest return asymmetry available in 2026.”

CHAPTER VI

PT EN

Competitive Advantage and *Positioning*.

Insurance is dominated by scale, loss ratio and actuarial quality. The winners are those who price better, operate more efficiently, and pay claims faster. FHE does not change that fundamental logic — but it allows competition on a new layer that competitors cannot easily replicate.

The three possible positionings

1 — The Insurer That Does Not Surveil You

Focus on direct communication with the policyholder. Explicit positioning as "the insurer that takes care of your risk without invading your privacy". Works best for premium and corporate segments where privacy is valued.

2 — The Sector Anti-Fraud Orchestrator

Focus on building an FHE anti-fraud consortium. Captures the role of sector organizer. Works for top 5.

3 — The Leader in UBI and Wellness

Focus on unlocking mass adoption of telematics and wellness with verifiable privacy. Works for insurers with a strong bet on personalization.

The cost of not positioning

The scenario to spell out: what happens if none of the large Brazilian insurers structurally adopts FHE in the next 36 months? Answer: **insurtechs will capture the space**. Lemonade, Justos, and new

entrants will offer "insurance with verifiable privacy" as a differentiator, capturing premium segments. In five years, the position will be taken.

CHAPTER VII

PT EN

The *24-Month* Roadmap.

01

MONTHS 1–6 · LEARN

Foundation and capability

Hire a founding crypto engineer. Identify three use cases (recommendation: collaborative fraud, UBI, wellness). Align with the Brazilian Insurance Regulator (SUSEP) and the Brazilian Data Protection Authority (ANPD).

02

MONTHS 7–14 · BUILD

Internal pilot

Build one end-to-end case. Recommendation: fraud detection under FHE for a segment (auto or health).

03

MONTHS 15–20 · FIRST COLLABORATION

Joint study with another insurer

Launch the first anti-fraud consortium with a partner insurer. Premium pricing for a new product category.

04

MONTHS 21–24 · INSTITUTIONAL CAPABILITY

Adoption as a pillar

Multiple cases. Launch of a wellness product under FHE. Public communication.

CHAPTER VIII

PT EN

Risks, Mitigations and *Pitfalls*.

1 · Inability to hire talent

Mitigation: acquisition via specialized consulting.

2 · Actuarial cultural resistance

Actuaries are conservative. **Mitigation:** show that FHE preserves model fidelity.

3 · Other insurers do not join the anti-fraud consortium

Mitigation: start with smaller insurers. Top 5 will follow.

4 · The Brazilian Insurance Regulator (SUSEP) does not understand the architecture

Mitigation: engage SUSEP early, in advisory mode.

5 · Computational cost at scale

Mitigation: hybrid architecture.

Pitfall 1 · Treating it as an IT project

FHE must report to the CRO or Chief Underwriting Officer.

Pitfall 2 · Starting with the most ambitious case

An inter-insurer consortium is politically complex. Start internally.

Pitfall 3 · Forgetting key governance

Who custodies the policyholder's key? A critical design.

PT EN

A letter to the next decade of *insurance*.

The industry you lead is one of the oldest that still exists. Insurance has existed longer than most countries, has crossed wars, revolutions and crises, and has endured because it offers something no other institution offers: the ability to transform individual risk into collective risk, and thereby make bearable what individually would be intolerable. This is the central promise, and it has been competently kept for centuries.

But the technology that sustains this promise is changing. The data that allows good pricing, fraud fighting, personalized product — that same data is now the industry's biggest regulatory and reputational liability. Every actuarial improvement is, on the other side, one more layer of risk. Every wellness feature is one more point of exposure. Every partnership with a hospital or pharmacy is one more legally delicate cross-reference.

It is possible to return to a form of robust fulfillment of the old promise without losing the benefits of modern technology. FHE allows you to continue offering accurate pricing, telematics, wellness, fraud fighting and intelligent reinsurance — **without ever decrypting the individual policyholder**.

What is at stake is not a technical feature. It is the possibility for the insurer to return, unambiguously, to being the institution that protects the policyholder rather than merely surveilling them.

> *"In three years, some insurer will lead. The question is whether it will be yours, or the one you will have to look at as a reference."*

There is a window. It is narrow. It is real. The rest is courage.

APPENDIX A

PT EN

Executive *Glossary*.

FHE

Computation over encrypted data.

PSI

Private Set Intersection. Central use case for collaborative fraud fighting.

UBI — USAGE BASED INSURANCE

Insurance priced by actual usage (e.g., pay-as-you-drive).

LOSS RATIO

Ratio of claims paid to premiums received. Central metric of actuarial efficiency.

SOLVENCY II

European solvency regime for insurers.

BRAZILIAN INSURANCE REGULATOR (SUSEP)

Superintendence of Private Insurance — Brazilian sector regulator.

RLWE

Mathematical foundation of modern FHE and NIST PQC.

LATTIGO, OPENFHE, CONCRETE

FHE libraries.

APPENDIX B

PT EN

Vendors and *Partners*.

VENDOR	FOCUS
Inpher	FHE+MPC, focus on finance and insurance
Duality	OpenFHE
Zama	Concrete, insurtech use cases
Tune Insight	Lattigo
Owkin	For insurers with a strong health presence
Stickybit	Brazilian technical boutique

APPENDIX C

PT EN

30 Questions for the *CRO/CUO/CFO*.

Strategy

1. Who understands advanced cryptography in our company?
2. What is our current exposure to sensitive data processing?
3. How many external vendors have access to policyholder data?
4. Inventory of cross-references with hospitals/pharmacies/banks?
5. Legal opinion on sustainability?

Priority use cases

6. How much do we lose annually to fraud we cannot fight alone?
7. How much would our loss ratio improve with richer models?
8. Why do UBI/wellness no longer take off?
9. Which consortia are missing in our sector?
10. Which reinsurers would accept encrypted data?

Technical

11. Which FHE scheme for our first use case?
12. Latency for real-time underwriting?
13. How do we integrate with the actuarial system?
14. How do we manage policyholder keys?
15. Is threshold cryptography compatible?

Cost

PT EN

16. FHE cost vs plaintext?
17. Build in-house or via vendor?
18. 24-month capex and opex?
19. C-level sponsor confirmed?

Regulation

20. Demonstrable LGPD / SUSEP compliance?
21. Actuarial models auditable under FHE?
22. Dialogue with the Brazilian Insurance Regulator (SUSEP)?
23. Communication to the policyholder?

Commercial

24. Would other insurers join an anti-fraud consortium?
25. How do we price products with FHE?
26. Which segments would pay for verifiable privacy?
27. What is the brand narrative?
28. Internal case study?
29. Worst-case scenario if a competitor announces first?
30. Are insurtechs already doing this?

PT EN

~

The Risk That Is Priced Without Being Seen

Strategic eBook for senior insurance management.
Volume I · Edition 2026 · Confidential distribution.

Set in Iowan Old Style and SF Pro.

— end —