PT EN

STRATEGIC EBOOK · EXECUTIVE LEVEL

FOR CEOS, CFOS, CHIEF MEDICAL OFFICERS, CHIEF RISK OFFICERS AND BOARD MEMBERS OF THE LARGEST BRAZILIAN AND GLOBAL HEALTH INSURANCE OPERATORS

The Claim That *Computes Itself*.

How Fully Homomorphic Encryption enables the operator to cross-reference data with hospitals, pharmacies and providers — without ever decrypting the patient — and finally make value-based care work.

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 health insurance operator sits at the center of the industry's oldest and hardest problem: how to pay the provider for value, not for procedure, without compromising the beneficiary's privacy. The entire value-based care discussion, the full arsenal of claims management, all the actuarial sophistication of the last decade hits the same obstacle: to make good decisions, the operator has to cross-reference data that lives in different silos (hospital, pharmacy, lab, clinic), and none of these parties can hand over nominal records without violating regulation or triggering contractual disputes.

The result is an industry that operates, simultaneously, under an excess and a scarcity of data. Excess, because every operator accumulates years of claims, authorizations, reports and costs in its systems. Scarcity, because most of that data is structurally unusable outside the silo where it was generated — real cross-referencing requires including hospitals and pharmacies, and every cross-reference requires months of DUAs, legal opinions and contractual distrust.

1

VBC STALLS WITHOUT CROSS-MATCHING

Paying for outcomes requires knowing the outcome. Knowing the outcome requires cross-matching with the hospital. Cross-matching requires a level of trust that does not exist today.

2

STRUCTURAL FRAUD

Industry estimate: 6–10% of medical expenses are fraud or waste. Fighting it requires cooperation among operators — today impossible.

3

BLIND ACTUARIAL

4

FHE IS MATURE

Risk models depend on real clinical data. Today, actuaries work with poor proxies because they cannot see individual data.

Use cases already in production at European payors. The technology is viable wi
IT budget of any top-20 operator.

PT EN

FHE — Fully Homomorphic Encryption — unlocks all of these cases. It allows the operator to cross-reference with the hospital without either side seeing the individual patient. It enables anti-fraud consortia between competing operators. It lets actuaries work on real encrypted clinical data. It makes value-based care contracts actually work.

> *"The next decade of the private health market will be defined by which operators manage to operate over cross-referenced data without violating the privacy of those who trust them with the most intimate part of their lives."*

THE DECISION

The board's question is not "whether" to invest in defensible data architecture. It is "who in your category will lead — and what is the cost of finding out it was someone else".

CHAPTER I

PT EN

The Operator as a *Data Policy*.

The modern operator accumulates one of the country's largest clinical-data assets — and nearly all of that asset is paralyzed by the very rules it upholds.

Every Brazilian health insurance operator running at national scale holds, in its systems, years of history for every beneficiary. Authorized procedures, hospitalizations, surgeries, tests, consultations, high-cost medications, complications, deaths. In volume and granularity, this archive is richer than any equivalent database in public research. It is also the central asset for any serious project in risk management, predictive actuarial work or value-based care.

And, at most operators, it is partially paralyzed. Regulation (rightly) prohibits secondary uses without a robust legal basis. Internal legal teams operate under a logic of absolute minimization. Every new data-use project takes months of review. Every cross-reference with a hospital or pharmacy requires a DUA negotiated bilaterally. The result is an industry that holds the best clinical data in the country and uses it only marginally.

The operator's invisible assets

PT EN

ASSET	WHAT IT IS	WHY IT IS UNIQUE
Longitudinal beneficiary history	Years of healthcare use with financial context	No hospital has this full temporal view
Care chain	Sequence of providers and procedures per episode	Lets you see the patient "journey"
Real costs	Price actually paid for each service	Only actor with full cost visibility
Prescribing behavior	Who prescribes what, with which pattern	Material for quality benchmarking
Adverse events by region	Concentration of complications by area	Early signal others lack
Fraud and waste	Anomalous usage patterns	Hard to fight alone

What Changed in the Value Chain

The operator has always been the financial intermediary between beneficiary and provider. What has changed in the last ten years is that this intermediation has also become an industrial-scale data operation. Every authorization generates an event. Every medical bill generates dozens. Every test generates a result. In some segments (oncology, advanced therapies, rare diseases), the data volume per beneficiary rivals that of a hospital.

Operators have begun investing in AI for authorization, in advanced actuarial models, in their own telemedicine, in chronic-disease management programs. Each of these operations increases the potential value of the data and simultaneously increases regulatory exposure.

THE SILENT PROBLEM

PT EN

The operator runs cross-references with hospitals and pharmacies that the Brazilian Health Insurance Regulator (ANS) and the Brazilian Data Protection Authority (ANPD) will, within a few years, regard as problematic. The current contracts work only because no one has yet been seriously audited. That will change.

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

CHAPTER II

PT EN

The Regulatory *Siege*.

The operator lives simultaneously under three regulatory layers: Brazilian Health Insurance Regulator (ANS), the Brazilian Data Protection Authority (ANPD), and the National Health Council (CNS) for clinical research where applicable. All three are tightening.

The comfortable illusion some operator boards still hold is that the relevant regulator is ANS, and LGPD (Brazilian data protection law) is a DPO matter. That was true in 2020. It is no longer. The intersection of ANS, ANPD and clinical-research regulation is becoming the most complex terrain in the entire operation.

LGPD and article 11

Health data is a special category. From LGPD's standpoint, the operator is a controller. Every cross-reference with a hospital, pharmacy or provider requires a specific legal basis. The "health protection" exceptions are interpreted narrowly. In 2025 the Brazilian Data Protection Authority (ANPD) opened formal investigations against operators regarding data use for telemedicine and predictive management.

ANS and the structural tension

The Brazilian Health Insurance Regulator (ANS) wants transparency, quality, fraud control, value-based care, reduced bill disputes. All of this demands more data use, more cross-matching. LGPD demands minimization. The two regulations pull in opposite directions. Operators live this tension without a technical tool to resolve it — until now.

HIPAA and the obsolescence of anonymization

Operators with U.S. operations (United, Cigna, Aetna) live under HIPAA. The traditional defense: Safe Harbor de-identification. Already invalidated by re-identification. HHS has opened multiple investigations.

EHDS and the emerging European standard

EHDS — European Health Data Space — will require technical capacity for privacy-preserving analytics. It is setting the technical standard that regulators worldwide will adopt in the next five years.

The conceptual shift

> *"Policy alone is not enough. Technical proof that individual data could not have been seen is required."*

FHE stops being a technical curiosity and becomes a structural defense tool. An operator that processes data under FHE can demonstrate to ANS, the Brazilian Data Protection Authority (ANPD), the beneficiary and the hospital partner that individual data was never accessible.

The cost of inaction

PT EN

RISK	PROBABILITY 5 YEARS	IMPACT
LGPD fine for cross-referencing without legal basis	High	2% of revenue or USD 50M+
Brazilian Data Protection Authority (ANPD) investigation over a vendor failure	Medium-high	Reputation + expensive remediation
Class action over medical-record exposure	Medium	Hundreds of millions
ANS transparency obligation impossible without FHE	Medium	Emergency implementation cost
Reputational crisis post-breach	Low-medium	Loss of premium book

CHAPTER III

PT EN

FHE in Executive *Language*.

No mathematics. What the board needs to understand.

Transparent vault. You see there is something inside, you do not see what it is. You manipulate the content from the outside — add, multiply, compare, run entire actuarial models — without ever opening it. It returns sealed. Only the key owner opens it. This is FHE.

The conceptual leap

All current cryptography protects data in transit (TLS) and at rest (AES). The third state — data in use, during processing — has always required plaintext. It is at that instant that an AI vendor needs to see beneficiary data. It is where the actuarial system runs over millions of claims in the clear. It is where the hospital cross-reference exposes both sides. **FHE eliminates the third state.**

How it works

> ANALOGY FOR THE OPERATOR
>
> The operator encrypts its beneficiaries' data with its own key. It sends the encrypted base to a neutral server (actuarial vendor, hospital partner, management platform). That server — which never receives the key — runs the entire computation (risk modeling, scoring, outlier identification) over the ciphertexts. It returns the encrypted result. Only the operator opens it. At no point did the vendor or the partner see an individual beneficiary.

FHE vs alternatives

PT EN

TECHNOLOGY	PROMISES	FAILS
De-identification	"We removed identifiers"	Trivial re-identification via linkage
TEE	"The chip isolates"	Trusts the manufacturer; side-channel attacks
Federated Learning	"Data stays local"	Gradients leak individual data
Differential Privacy	"We added noise"	Poor for decisions about an individual beneficiary
FHE	**"Server never sees in plaintext"**	**High computational cost — but decreasing**

The cost myth

For a top-20 operator with revenue above USD 5B, total investment in FHE lands below 0.3% of the IT budget. It is less than many operators spend on a single authorization-system migration. And the typical case closes on a single successful value-based care contract alone.

CHAPTER IV

PT EN

Use Cases by *Line*.

VBC, fraud, actuarial, cross-matching, authorization, telemedicine.

Value-based care that finally works

VBC is the decade's obsession, and the central reason it almost never works is simple: outcome-based contracts require tracking the beneficiary over time, across multiple providers, with mutual transparency. The operator needs to know the clinical outcome to pay; the hospital needs assurance that the operator will not use the data for indirect bill disputes; the beneficiary needs privacy respected. The three requirements, in traditional architectures, are incompatible.

Under FHE: the operator encrypts the claims base, the hospital encrypts the clinical-outcome base, both contribute to a neutral server that computes the cross-reference and returns only the aggregated outcome metric (complication rate, readmission, survival). Payment runs on the metric. **Neither side needs to see the other's individual data.**

Collaborative fraud fighting

Fraud and waste cost the sector between 6% and 10% of medical expenses — billions annually. Effective response requires cooperation among competing operators: detecting providers who bill the same procedure across multiple operators, beneficiaries with anomalous usage patterns, doctors with out-of-pattern prescribing rates. Today this cooperation is structurally impossible — competitors do not share data for competitive and legal reasons.

Under FHE with Private Set Intersection (PSI): operators encrypt lists of providers, beneficiaries or patterns, and discover **only the intersection**. Without revealing the underlying bases. **This unlocks billions in sector-wide savings that today literally do not exist.**

Predictive actuarial on real clinical data

Actuaries today work mainly with financial data and health proxies (demographics, plan type, usage history). They do not work with medical records because it is legally prohibited. Under FHE, actuarial models can run over encrypted clinical data — including data coming from the hospital's medical record. **Risk pricing becomes dramatically more accurate**, and the operator stops cross-subsidizing bad books with good ones.

Pharmacy cross-matching for adherence management

The operator wants to know whether a chronic beneficiary is adhering to treatment. The pharmacy knows. Cross-referencing nominally is legally complex. Under FHE: both encrypt, the adherence management system runs over the encrypted cross-reference and returns non-adherence alerts without either side seeing the individual beneficiary. The operator intervenes (call, reminder, offer of teleconsultation). Result: **avoided hospitalizations and reduced cost.**

Smart authorization with beneficiary protection

Authorization of high-cost procedures is the operation's highest-friction point. Predictive models can help decide but require plaintext individual data. Under FHE, the authorization model runs over the beneficiary's encrypted data, and the decision is produced without the central system seeing the individual clinical history. **Auditing becomes more robust** because the process is mathematically verifiable.

In-house telemedicine

Operators are investing in internal telemedicine as a competitive differentiator and cost lever. This entire operation involves beneficiary clinical data flowing through proprietary systems. Under FHE, the beneficiary's history stays encrypted, and the professional sees only what is needed for the consultation — without persistence in central systems.

RWE for pharma partnerships

The operator holds real-world drug usage data that pharma would pay dearly to have. Today, this market is partial and legally fragile. Under FHE, the operator can offer an "encrypted query" as a product: pharma sends a query, the operator computes over the encrypted base, returns aggregate statistics. **A new recurring revenue market.**

Quality monitoring across providers

The operator wants to compare quality across accredited hospitals — readmission rate, complications, adjusted mortality. Hospitals resist because they fear public rankings. Under FHE: hospitals encrypt, an aggregator computes percentiles, each hospital sees its relative position without seeing the others' absolute numbers. The operator gains real quality visibility for accreditation decisions.

CHAPTER V

PT EN

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

Initial capex

COMPONENT	INVESTMENT
Founding team (crypto + ML + actuarial + legal)	USD 5M – 8M / year
Licenses	USD 300k – 1M / year
Compute infrastructure	USD 2M – 4M initial
Strategic consulting	USD 1M – 2.5M
Regulatory study	USD 500k – 1.5M
Integration with authorization, claims, actuarial systems	USD 2M – 5M
Total year 1	**USD 11M – 20M**

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**

The return — six vectors

1. Reduction of fraud and waste

6–10% of medical expenses is fraud/waste. For an operator with USD 5B in claims, this is USD 300–500M of annual exposure. Capture via inter-operator PSI: **USD 50–150M annually**.

2. Functional VBC

Well-implemented VBC contracts reduce total cost by 8–15%. For a top-20 operator: **USD 100–400M annually within five years**.

3. More accurate actuarial

Actuarial models on real clinical data reduce cross-subsidy between books. Estimate: **USD 30–100M annually**.

4. Chronic adherence

Avoided hospitalizations from better adherence: each adherent chronic patient is worth USD 500–2000/year. **USD 50–150M annually**.

5. RWE for pharma

New recurring revenue: **USD 30–100M annually**.

PT EN

6. Regulatory risk reduction

Hedge: **USD 20–80M in insured value**.

Business case

~USD 15M YEAR 1 INVESTMENT	~USD 11M STABILIZED ANNUAL OPEX
USD 500M+ VALUE ENABLED OVER 5 YEARS	30×–50× EXPECTED 5-YEAR ROI

> *“For any top-20 operator, FHE is the digital transformation investment with the highest return asymmetry available in 2026.”*

CHAPTER VI

PT EN

Competitive Advantage and *Positioning*.

The private health industry is dominated by consolidation and the relentless pursuit of lower claims ratios. Whoever runs cheaper wins. FHE does not change that fundamental logic — but it allows reducing claims in a way competitors cannot replicate.

The three possible postures

Posture 1 — The Operator Leading in Real VBC

Focus on outcome-based contracts that truly work. Positioning as "the operator that pays providers for delivered, proven value, without exposing the beneficiary". Works best for operators with strong corporate presence.

Posture 2 — The Operator Defending the Beneficiary

Focus on direct communication with premium beneficiaries. Public program around data protection. Positioning as "the operator you trust". Works for operators with mid-high and premium books.

Posture 3 — The Sector Anti-Fraud Convener

Focus on building an anti-fraud consortium with other operators. Captures the convener role, gains ANS visibility, reframes the sector narrative. Works for top-5 operators with political muscle.

The cost of not taking a position

The scenario to make explicit: what happens if none of the large operators adopts FHE structurally in the next 36 months? Answer: **healthtechs will capture the space**. FHE-based risk management

platforms will emerge, offering services to smaller operators and draining margin from the large ones. Within five years, the position will be taken.

CHAPTER VII

PT EN

24-Month *Roadmap*.

01

MONTHS 1–6 · LEARN

Foundation and capability

Hire a founding crypto engineer or partner with a consultancy. Identify three use cases (recommended: VBC pilot, collaborative fraud, chronic adherence). Align with legal and the DPO.

02

MONTHS 7–14 · BUILD

Internal pilot

Build one use case end-to-end. Recommendation: VBC pilot with a single trusted hospital partner. Validate latency, integration with TASY/MV, key governance.

03

MONTHS 15–20 · FIRST COLLABORATION

Joint study with hospital

Launch the first real VBC contract or cross-reference with a provider using FHE. Marketing aimed at HR at corporate clients. Premium pricing versus the traditional product.

04

MONTHS 21–24 · INSTITUTIONAL CAPABILITY

Adoption as a pillar

Multiple contracts under FHE. Possible first anti-fraud consortium with other operators. Structured public communication.

CHAPTER VIII

PT EN

Risks, Mitigations and *Pitfalls*.

1 · Inability to hire talent

High probability. **Mitigation:** partnership with a specialized consultancy.

2 · Hospital partner resistance

Hospitals resist collaborating with operators even under FHE — historical distrust. **Mitigation:** start with a hospital where there is an existing trust relationship and a VBC contract already running.

3 · Integration with legacy systems

A typical operator runs dozens of systems. **Mitigation:** integrate only what is necessary for the first case.

4 · Competing operator declines anti-fraud consortium

Competitors may resist even under FHE. **Mitigation:** start with smaller operators where the gain is greater. Bigger players follow later.

5 · ANS interprets it as excess data collection

Unlikely, but possible. **Mitigation:** engage ANS from day one.

Pitfall 1 · Treating it as an IT project

FHE should report to the Chief Medical Officer or Chief Risk Officer, not the CIO.

Pitfall 2 · Starting with an ambitious VBC

VBC with multiple hospitals simultaneously is politically too complex to start with. Start with one hospital, validate, expand.

Pitfall 3 · Underestimating the hospital partner relationship

PT EN

FHE reduces technical friction, not human friction. The hospital relationship must be cultiv
parallel.

A letter for the next decade of *private healthcare*.

For the CEOs, Board Members and Chief Medical Officers of operators that can still choose to lead.

The operator you lead was built on an old promise: that it is possible to organize healthcare in a way that combines access, quality and financial sustainability. That the intermediary between patient and provider, when well run, improves the experience of all. That the beneficiary who entrusts their health to an operator is making a reasonable pact: I pay, you manage, and if I get sick, you take care of me.

This promise has lasted for decades. It survived the credibility crisis of the 1990s, ANS regulation, the consolidation of the 2000s, the regulatory pressure of the last ten years. It survived because it was — and largely still is — true. Beneficiaries who choose one premium operator over another do so, at heart, out of institutional trust in the promise of care.

But in the last fifteen years, without anyone decreeing it, the relationship between operator and beneficiary has changed in nature. The beneficiary stopped being someone who signs a contract and uses it when needed. They have become a continuous source of clinical, behavioral and financial data. Every healthcare use generates records. Every authorization generates analysis. Every accredited hospital adds a layer of cross-matching that no one individually can audit.

It is possible to turn back without losing the benefits. FHE allows the operator to keep running VBC, predictive actuarial, adherence management and fraud prevention — **without ever decrypting the individual beneficiary**. It is possible to keep doing everything the modern operator needs to do. It is possible to do it while the institution keeps, with mathematical proof, that every beneficiary was respected.

What is at stake is not a technical feature. It is the possibility for the operator to become again, unambiguously, what it has always claimed to be: an institution that takes care of people at moments of vulnerability, with financial competence and clinical respect.

PT EN

> *“Within three years, some operator will lea*
> *The question is whether it will be yours, or the one you will have to look to as a reference.”*

There is a window. It is short. It is real. Whoever reads this eBook holds a map. The rest is courage.

APPENDIX A

PT EN

Executive *Glossary*.

FHE

Cryptography that allows computing over encrypted data without decrypting it.

PSI — PRIVATE SET INTERSECTION

Lets two operators discover shared providers or beneficiaries without revealing their bases. Central to collaborative fraud fighting.

VBC — VALUE-BASED CARE

Remuneration model based on clinical outcomes instead of procedures.

RWE — REAL WORLD EVIDENCE

Clinical evidence derived from real-world usage data.

LGPD ART. 11

Special category — health.

ANS, ANPD, CNS

The three converging regulators the operator must answer to.

THRESHOLD CRYPTOGRAPHY

Distribution of a key across multiple parties with a required quorum.

LATTIGO, OPENFHE, CONCRETE

Main FHE libraries.

APPENDIX B

PT EN

Vendors and *Partners*.

VENDOR	FOCUS
Tune Insight	Lattigo, focus on multi-institution health
Owkin	FL+FHE for clinical research
Inpher	FHE+MPC for finance and health — historically strong with payors
Duality	OpenFHE
Zama	Concrete
Stickybit	Brazilian technical boutique

APPENDIX C

PT EN

30 Questions for the *Chief Medical Officer and CFO*.

Strategy

1. Who in our company understands advanced cryptography?
2. What is our current exposure to beneficiary data processing?
3. How many external vendors have technical access?
4. Do we have an inventory of which data we cross-reference with hospitals/pharmacies today?
5. Legal opinion on the sustainability of the architecture?

Priority use cases

6. Which VBC contracts are paralyzed today by technical incapacity?
7. How much do we lose yearly to fraud we cannot fight alone?
8. How much cross-subsidy exists between books due to imprecise actuarial?
9. How many avoidable hospitalizations happened due to poor adherence?
10. Which hospital partnerships are currently fragile?

Technical

11. Which FHE scheme for our first case?
12. Acceptable latency?
13. How do we integrate with authorization and claims systems?
14. How do we manage keys across operator, hospital and beneficiary?
15. Is threshold cryptography compatible?

Cost

PT EN

16. Cost per FHE analysis vs plaintext?
17. Build in-house or via vendor?
18. Capex and opex over 24 months?
19. C-level sponsor confirmed?

Regulation

20. Demonstrable LGPD and ANS compliance?
21. DPO engaged?
22. Dialogue with ANS and the Brazilian Data Protection Authority (ANPD)?
23. Communication to beneficiaries?

Commercial

24. Are hospitals willing to run VBC under FHE?
25. Would other operators join an anti-fraud consortium?
26. Will pharma pay for FHE-based RWE?
27. Differentiated pricing for FHE-backed services?
28. How will we communicate publicly?
29. Internal case study?
30. Worst-case scenario if a competitor announces first?

PT EN

~

The Claim That Computes Itself

Strategic eBook for the senior leadership of health insurance operators.
Volume I · Edition 2026 · Confidential distribution.

Set in Iowan Old Style and SF Pro.

— end —