PT EN

STRATEGIC EBOOK · EXECUTIVE LEVEL

FOR CEOS, CDOS, COMMERCIAL DIRECTORS AND BOARD MEMBERS OF THE LARGEST BRAZILIAN AND GLOBAL PHARMACY CHAINS

The Pharmacy that Never *Remembers*.

How Fully Homomorphic Encryption enables the large pharmacy chain to monetize data, fight fraud and build a clinical loyalty program — without ever seeing the individual patient.

VOLUME I · EDITION 2026 · CONFIDENTIAL

TABLE OF CONTENTS

PT EN

What you will *read*.

Executive decision document. Written to be read in an executive meeting or on a Saturday morning before a decision about the future of the chain's data.

IX Manifesto

For CEOs of chains that can still choose to lead

PT EN

· Appendices

PT EN

The argument in *one* page.

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

The large pharmacy chain is, today, one of Brazil's largest hubs of sensitive clinical data — and almost no one in the leadership of these chains thinks of them that way. Every taxpayer ID (CPF) registered in a loyalty program carries a medication history that, read by someone who knows how to read it, tells the patient's clinical story: hypertensive, diabetic, under psychiatric treatment, on chemotherapy, on hormone replacement therapy, on antiretrovirals. In practice, the pharmacy is an outpatient record running parallel to SUS and private health — only without equivalent governance.

This position is an extraordinary strategic asset. It is also a growing regulatory liability that has not yet been priced. The three major pressures converge:

1

LGPD TIGHTENING

In 2025 the Brazilian Data Protection Authority (ANPD) began investigating secondary use of pharmacy data without a robust legal basis. It will be the first of many.

2

PHARMA WANTS DATA

The RWE market surpassed USD 5B globally. The pharmacy is a natural source — but only if it can sell without exposing the patient.

3

STRUCTURAL FRAUD

"Doctor shopping" and fake prescriptions cost the sector billions. Fighting it requires

4

POOR ADHERENCE

Non-adherence to chronic treatment causes 30% of avoidable hospitalizations. The pharmacy knows — and cannot act.

cooperation between chains — today impossible.

PT EN

FHE — Fully Homomorphic Encryption — allows the chain to unlock all these cases without ever decrypting the customer's individual data. Pharma buys encrypted insights. Chains detect fraud collaboratively without exposing their bases. Adherence programs work without the central algorithm ever seeing the individual history. All of this is mathematically possible today, and operationally viable within the IT budget of any chain with more than a thousand stores.

> *"The next decade of pharmacy retail will be defined by which chains manage to monetize clinical data without betraying the customer who trusts them with the most intimate part of their life."*

THE DECISION

The question for the board is not "whether" to invest in defensible data architecture. It is "who in your category will lead — and what is the cost of waiting until you find out it was someone else".

CHAPTER I

PT EN

The Counter *Industry*.

The pharmacy has quietly become one of Brazil's largest hubs of sensitive clinical data. Almost no one thinks of it this way — and this institutional blindness is the sector's biggest risk and biggest opportunity.

In 2005, a customer walked into the pharmacy, showed a prescription, bought the medicine and left. The register held a name, a taxpayer ID and an address. That was it. In 2025, the same customer opens the chain's app, receives reminders to refill her medication, earns points in the loyalty program, has a teleconsultation with a pharmacist, receives product suggestions based on purchase history, and has her entire medication pattern stored for years in servers that cross-reference data with at least half a dozen external providers.

This transformation happened without any decree. It was built by successive features, each defensible in isolation, each adding a fraction of collection. The aggregate result — which no one planned — is an industrial-scale sensitive clinical data operation, mediated by a network of IT vendors no one fully controls, under regulation that is still forming, with accumulated reputational risk no one has yet priced.

What Changed in the Value Chain

Pharmacy has always been retail. What has changed is that five new operations were layered on top of retail, each with its own technical and legal complexity:

OPERATION	WHAT IT IS	RISK
Clinical loyalty program	Purchase history cross-referenced with health profile	Special category under LGPD art. 11
Pharmacist teleconsultation	Clinical care via app	Regulated by CFF; clinical liability
Sales to pharma	Aggregated insights on drug usage	Fragile de-identification; dubious regulatory value
Cross-matching with health plans	Adherence, complications, cost	Bilateral cross-matching without robust legal basis
Controlled substances and the National Drug Tracking System (SNGPC)	White/blue/yellow prescriptions, retention	Brazilian Health Authority (ANVISA) + CFM; fraud and exposure risk

The chain's invisible assets

It is important to name what is at stake. A large Brazilian pharmacy chain accumulates, over five years of digital operation, a set of assets whose scientific and commercial density is virtually unparalleled:

- **Longitudinal medication history** — millions of patients followed for years, with purchase patterns, abandonment, brand switching
- **Geography of disease** — where, in which city or neighborhood, which clinical condition is growing
- **Real adherence** — unlike self-reported adherence in consultation, the pharmacy knows when the patient actually bought
- **Prescribing patterns** — who prescribes what, in which dose, with which frequency
- **Sentinel events** — when a patient stops buying (abandonment or complication)
- **OTC behavior** — self-medication as a proxy for undiagnosed symptoms and disease

Nearly none of this can be used without massive friction. This is the central contradiction of pharmacy retail in 2026: **there has never been so much data available, and it has never been so risky to try**

to use it.

PT EN

What no one told the customer

The customer who registers their taxpayer ID in a loyalty program does not understand, in any practical sense, what they are handing over. They believe they are trading an identifier for a discount. They are, at the same time, authorizing that their medication be stored, cross-referenced, analyzed, potentially sold to pharma, potentially shared with a health plan. The terms of use say so in some way. But saying is not understanding, and the industry operates over that difference.

> **THE SILENT PROBLEM**
>
> The current operation depends on a chain of trust between customer, pharmacy, technology vendor, pharma platform and cloud that has dozens of points where data exists in plaintext. Regulation is, finally, starting to count the points.

“The question for the chain's board is not whether the current data architecture is sustainable. It is how long until the first public lawsuit changes everything.”

CHAPTER II

PT EN

The Regulatory *Siege*.

The regulation governing pharmacies has always been heavy, but until five years ago it was heavy in the wrong dimension. Now it is starting to tighten exactly where it hurts.

A comfortable perception is shared by much of chain leadership: that the regulation that matters is the Brazilian Health Authority (ANVISA) regime on dispensing, and that customer data is a marketing department matter. This view worked in 2024. It does not work in 2027. And whoever accepts it as truth will be surprised by changes already underway.

LGPD and article 11

Health data is a special category under LGPD (Brazilian data protection law). A pharmacy, by recording a medication history in the customer's name, is a controller of this category. Article 11 requires a specific and robust legal basis for any processing. The "health protection" exceptions are interpreted narrowly. In 2025 the Brazilian Data Protection Authority (ANPD) opened the first formal investigation against a large Brazilian chain for data sharing with a marketing vendor without a demonstrable legal basis. It will be the first of many.

The detail few chains have internalized: responsibility for the data **does not end when it is shared with a vendor**. If the CRM vendor, the loyalty platform or the teleconsultation system leaks, the chain is jointly liable. The entire vendor chain has become a source of systemic risk.

ANVISA RDCs and the National Drug Tracking System (SNGPC)

The National Drug Tracking System (SNGPC) is the basis for oversight of white, blue and yellow prescriptions. The Brazilian Health Authority (ANVISA) has been systematically expanding traceability requirements. Every new RDC adds storage, retention and audit obligations. When these obligations

meet LGPD, tension appears: ANVISA wants perfect tracking, LGPD wants minimization. The two requirements are technically contradictory in traditional architecture. Under FHE, they no l

CFF and pharmacist teleconsultation

The Federal Pharmacy Council (CFF) has been regulating pharmacist teleconsultation as a professional act. The chain's entire "digital pharmacist" operation is under CFF scrutiny. The pharmacist's technical responsibility creates a new layer of exposure: if the chain offers clinical guidance via app, there is a responsible pharmacist, and there is real medical-legal risk.

GDPR, EHDS and why they matter even in Brazil

Brazilian chains with European operations (Alliance Boots/Walgreens, partnerships with global pharma) already face GDPR requirements. EHDS — the European Health Data Space — will require technical capability for privacy-preserving analytics as a prerequisite to participate in any initiative involving European patient data. EHDS defines the technical standard global regulation will adopt in the next five years.

The conceptual shift

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

Here FHE stops being a curiosity and becomes a defensive tool. The chain that processes data under FHE can demonstrate to the Brazilian Data Protection Authority (ANPD), CFF, the Brazilian Health Authority (ANVISA), the distrustful patient and the pharma partner that individual data was never accessible — not by employees, not by vendors, not by the cloud.

The cost of inaction

PT EN

RISK	PROBABILITY 5 YEARS	IMPACT
LGPD fine for sharing 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 medication exposure	Medium	Hundreds of millions
Loss of contracts with global pharma	Medium	USD 20M–100M annually
Reputational crisis post-breach	Low-medium	12–24 months of loyalty decline

CHAPTER III

PT EN

FHE in Executive *Language*.

No mathematics. No jargon. What the board needs to understand to make a decision.

Imagine a transparent safe. You can see there is something inside, but you cannot see what it is. Now imagine you can manipulate the contents from outside the safe, with mathematical gloves: add, multiply, compare, run regressions. You execute operations on the safe's contents without ever opening it. When finished, you return the sealed safe to the key owner, who opens it and sees the result. This is FHE.

The conceptual leap

All the cryptography your chain uses today — TLS in the app, AES in backups, HTTPS on APIs — protects data in *two* of the three states: in transit and at rest. The third state, "in use" (when the server processes), requires plaintext. It is in that state that a CRM vendor needs to see the history to generate the campaign. It is where the loyalty platform accesses taxpayer IDs to calculate points. It is where the BI tool runs queries over millions of transactions. **FHE eliminates the third state.**

How it works

> ANALOGY FOR THE CHAIN
>
> The chain locks its customers' data in a mathematical box using a key that only it holds. It sends the box to a neutral server (AI vendor, pharma platform, adherence partner). That server — which never receives the key — runs the analysis over the sealed box. The result comes back in another sealed box, which only the chain opens. Pharma paid for the insight; the vendor processed it; the customer was never exposed.

FHE vs alternatives

PT EN

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

The cost myth

FHE has dropped two to three orders of magnitude in seven years. For a chain with revenue above USD 5B, total investment — initial capex plus annual opex — lands below 0.3% of the IT budget. It is less than most chains spend on a single store-management system upgrade. And the use case typically closes on a single pharma contract.

CHAPTER IV

PT EN

Use Cases by *Line*.

What concretely changes in each operational vertical. Loyalty, fraud, pharma, adherence, controlled substances, OTC.

Clinical loyalty program

This is the category where the chain has the highest potential value and highest current exposure. The loyalty program today is mediated by a vendor that needs to see the purchase history to calculate points, segment campaigns, offer personalized discounts. Each of these operations exposes the customer.

1. PERSONALIZATION WITHOUT PERSISTENT PROFILING

Under FHE, the customer profile stays permanently encrypted on the server. The recommendation algorithm runs over ciphertexts. The campaign is generated without the chain or vendor ever seeing the customer list or what they bought. **The customer receives a relevant offer; the chain never had a readable profile to leak.**

2. REFILL REMINDERS WITHOUT REVEALING THE MEDICATION

The app reminds the customer to buy chronic medication before it runs out. This service is expensive today because it requires knowing which medication each customer takes. Under FHE, the reminder algorithm runs over the encrypted history. The central server never knows the customer takes an antidepressant. **The service is the same; the liability disappears.**

Collaborative fraud detection between chains

This is a case where FHE unlocks something *no other solution* can unlock. Fake prescriptions, doctor shopping (a patient collecting prescriptions from several doctors for the same controlled substance), antibiotic misuse, dangerous self-medication — all of this costs the sector billions annually. Fighting it requires cooperation between competing chains. Today, such cooperation is structurally impossible: chains do not share data for competitive and legal reasons.

Under FHE with Private Set Intersection (PSI), chains can encrypt taxpayer-ID lists of controlled-substance buyers and discover **only the intersection** — who appears at three or more chai simultaneously buying the same controlled substance. Without revealing entire bases. Wit revealing individual history. Only the fraud signal. **This is sector defense that literally does not exist today.**

Aggregated insights for the pharmaceutical industry

Pharma wants to buy pharmacy data to understand real-world drug usage, disease patterns, treatment effectiveness, regional market share. Today, this market exists via anonymized data (IQVIA/Close-Up model) — legally fragile and increasingly contested.

Under FHE, pharma sends an encrypted query ("how many patients in São Paulo started metformin in the last 90 days and abandoned it within 30?"). The chain computes over the encrypted base. It returns only the encrypted aggregate statistic, which pharma decrypts with its own key. Pharma paid for the insight. The chain booked revenue. The customer was never exposed. **It is a new recurring-revenue market with none of the legal risks of today's model.**

Chronic-adherence programs

Non-adherence to chronic treatment is responsible for 30% of avoidable hospitalizations. The pharmacy is the only institution that knows when the patient actually stopped buying — before the doctor knows, before the health plan knows. But acting on that information requires processing clinical data nominally — which regulation makes difficult.

Under FHE, the system detects abandonment, generates an intervention (reminder, a pharmacist call, teleconsultation offer), all over encrypted data. The central algorithm never knows the patient is José da Silva — it knows only that *some* patient in the "diabetic on metformin" segment has not bought in 45 days. The pharmacist making the call sees only what is needed during the call, and nothing persists afterward.

Cross-matching with the health plan

The operator has the patient's clinical history. The pharmacy has the medication history. Cross-matching nominally is scientific gold — and legally almost impossible. Under FHE, both parties encrypt their bases, execute an encrypted join on a neutral server, and only the aggregate result is decrypted. Non-

adherence detection, drug-interaction alerts, prevention of adverse events. **This reduces hospitalizations — and the operator pays for that.**

Controlled substances and SNGPC under cipher

The Brazilian Health Authority (ANVISA) wants perfect tracking of controlled substances. LGPD wants minimization. Traditionally, that is tension. Under FHE, it is possible to operate an encrypted National Drug Tracking System (SNGPC): the chain holds the data, ANVISA enforcement can run aggregate analyses (volumes, regions, anomalous patterns) over the ciphertexts without needing to access the individual patient. Traceability is maintained, privacy is mathematically guaranteed.

OTC and early disease detection

Over-the-counter purchase patterns (analgesics, antacids, antihistamines) are proxies for symptoms and undiagnosed disease. At scale, they become a public-health tool: a spike in fever medication in one region is a signal of a respiratory epidemic weeks before the health system officially detects it. Under FHE, the chain can offer this signal to a health authority or health partners without exposing individual customers.

Generics vs brand · analysis under cipher

Analysis of brand switching, loyalty to active ingredients, post-promotion behavior. All of this is valuable insight for pharma and for the chain to optimize its mix. Under FHE, the analysis happens without anyone accessing the individual history.

CHAPTER V

PT EN

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

The real numbers. How much it costs, how much it returns.

Initial capex

COMPONENT	INVESTMENT
Founding team (crypto + ML + PM + legal)	USD 4M – 6M / year
Licenses and tooling	USD 200k – 800k / year
Compute infrastructure	USD 1M – 2.5M initial
Strategic consulting	USD 600k – 1.5M
Regulatory study	USD 300k – 800k
Integration with POS, ERP, CRM, app	USD 1.5M – 4M
Total year 1	**USD 7M – 14M**

Annual opex

PT EN

ITEM	ESTIMATE
Compute	USD 1.5M – 4M
Maintenance team	USD 3.5M – 6M
Audit	USD 400k – 1M
Stabilized annual opex	**USD 5.4M – 11M**

For a chain with revenue above USD 5B (RD/Drogasil, DPSP, Pague Menos), this represents between **0.1% and 0.3% of revenue**. Less than most chains spend on a single national campaign.

The return — six vectors

1. New revenue from pharma under FHE

The RWE market for pharma is USD 5B globally today. A Brazilian chain with FHE captures a premium segment estimated at **USD 30M–150M in incremental annual revenue within three years**.

2. Reduction of collaborative fraud

Sector fraud estimate: 3–5% of controlled-substance sales. For a USD 10B chain with 8% in controlled substances, that is USD 24–40M of annual exposure. Reduction via inter-chain PSI: **USD 8–20M annually**.

3. Adherence program paid for by the operator

Operators pay for interventions that reduce hospitalizations. Each adherent chronic patient is typically worth USD 200–500/year to the payer. The chain can capture a share. Estimate: **USD 15–60M annually**.

PT EN

4. Reduction of regulatory risk

Expected fine exposure: USD 30–100M NPV over 5 years. Hedge: **USD 12–50M in insure**

5. Loyalty premium

Loyalty programs with verifiable privacy have 15–25% higher adoption and retention. For a chain with 50M registrations, the revenue impact per customer is measurable: **USD 20–80M annually**.

6. Advantage in strategic partnerships

Operators, hospitals and healthtechs prefer partners who demonstrate data protection capability. Access to exclusive partnerships: **USD 10–40M annually**.

Business case

~USD 10M YEAR 1 INVESTMENT	~USD 8M STABILIZED ANNUAL OPEX
USD 100M+ VALUE ENABLED OVER 5 YEARS	10×–25× EXPECTED 5-YEAR ROI

PT EN

“For any chain with more than a thousand stores, FHE is the digital transformation investment with the highest return asymmetry available in 2026.”

CHAPTER VI

PT EN

Competitive Advantage and *Positioning*.

FHE in pharmacy is about becoming the first chain that can say, with mathematical proof: "we care without invading".

The Brazilian pharmacy retail industry has, for twenty years, been dominated by consolidation, price and logistics. Whoever has more stores, better price, better delivery wins. That game continues. But a new layer of competition is emerging — and whoever positions themselves first captures an advantage that lasts a full decade.

The three possible postures

Posture 1 — The Chain That Cares Without Invading

Focus on direct communication with the customer. Public program on data protection. Annual external audit published. Explicit positioning as "the chain you can trust with your medication". Works best for premium/medical chains (where customers are more aware).

Posture 2 — The Defensible Health Platform

Focus on partnerships with pharma, operators and hospitals. Positioning as "the country's most trustworthy health data infrastructure". Recurring data revenue becomes a pillar. Works for large chains aiming to become platforms.

Posture 3 — Anti-Fraud Leader

Focus on organizing an anti-fraud consortium using PSI/FHE. Captures the sector convener role, gains visibility with the Brazilian Health Authority (ANVISA) and the Brazilian Data Protection Authority

(ANPD), reshapes public discourse on controlled substances. Works for any chain with a sponsor willing to invest political capital.

The cost of not taking a position

The scenario to make explicit: what happens if none of the large Brazilian chains adopts FHE structurally in the next 36 months? Answer: **healthtechs and pharma platforms will capture the space**. They will offer "anonymized pharmacy data" as a product, capturing margin that could be the chain's and exposing the chain to breach risk. Within five years, the position will be taken — and expensive to reverse.

> *"The chain leading FHE is not adopting technology. It is protecting the customer who trusts it with the most intimate part of their life."*

CHAPTER VII

PT EN

24-Month *Roadmap*.

01

MONTHS 1–6 · LEARN

Foundation and capability

Hire a founding crypto engineer or partner with a specialized consultancy. Identify three candidate use cases. Align with legal and the DPO.

Output: documented architecture, three selected cases, favorable legal opinion.

02

MONTHS 7–14 · BUILD

Internal pilot

Build one use case end-to-end. Recommendation: an adherence program under cipher (high value, low operational risk). Validate latency, integration with ERP/CRM/POS.

Output: functional demo, validated metrics, first customer group in beta.

03

MONTHS 15–20 · FIRST B2B CLIENT

First contract with pharma under FHE

Launch the commercial offer to a pharma partner — encrypted query over the base. Marketing aimed at Medical Affairs and RWE teams at global pharma. Premium pricing versus the traditional IQVIA product.

Output: first contract closed, first insight delivered, first attributable revenue.

04

MONTHS 21–24 · INSTITUTIONAL CAPABILITY

Adoption as a strategic pillar

Multiple use cases on the infrastructure. Public customer program. Possible first anti-fraud consortium with other chains.

Output: 3+ active cases, first inter-chain consortium, sector recognition.

CHAPTER VIII

PT EN

Risks, Mitigations and *Pitfalls*.

1 · Inability to hire talent

High probability. **Mitigation:** partnership with a specialized consultancy (Stickybit, Tune Insight). The chain does not need talent in-house from day one.

2 · Internal cultural resistance

Retail operations are averse to technical complexity. **Mitigation:** treat it as a commercial project, not an IT one. Engage the Commercial Director and CDO from day one. Communicate in business language.

3 · Integration with legacy systems

A typical chain runs dozens of systems (POS, ERP, CRM, app, loyalty, BI). **Mitigation:** integrate only the 2–3 that matter for the first case.

4 · Computational cost for high volume

Some operations (queries over an entire base of 50M customers) are still expensive. **Mitigation:** start with selective high-value-per-query cases.

5 · Pharma resisting the new model

Pharma already has relationships with IQVIA. It may resist change. **Mitigation:** offer FHE as a complement, not a replacement. Start with Medical Affairs where privacy sensitivity is higher.

6 · Competitor announces first

Mitigation: speed. Every month of delay is a month of risk.

Pitfall 1 · Treating it as an IT project

PT EN

FHE should report to CDO/Commercial, not CIO. Otherwise: technical delivery without co
capability.

Pitfall 2 · Starting with the most ambitious case

Trying to start with the inter-chain anti-fraud consortium (politically complex). Mistake. Start internally, validate, expand.

Pitfall 3 · Forgetting key governance

Who is the key custodian? Customer? Chain? The Brazilian Health Authority (ANVISA)? CFF? Key-governance design is half the project.

A letter for the next decade of *pharmacy retail*.

For the CEOs, Board Members and CDOs of chains that can still choose to lead.

The chain you lead grew on a simple, old promise: that the pharmacy is a place where a customer can arrive in a moment of need and be served with competence, respect and privacy. That the pharmacist behind the counter is a trustworthy professional. That the chain's brand is worth more than the price at the neighboring store because it carries decades of a relationship built one purchase at a time.

This promise has lasted for decades. It survived consolidation, standardization, POS digitization, the arrival of e-commerce. It survived because it was — and largely still is — true. Customers who choose to buy at a premium chain instead of the neighborhood drugstore do so, at heart, out of institutional trust.

But in the last fifteen years, without anyone decreeing it, the relationship between chain and customer has changed in nature. The customer stopped being the person who shows up at the store and leaves with a bag of medicine. They have become a continuous source of data: taxpayer ID, purchase history, loyalty app, store geolocation, consumption patterns, teleconsultation data. Each of these data points was born from a defensible feature. The aggregate result is an operation no individual executive would consciously design: massive collection of intimate clinical data, mediated by dozens of technology vendors, under regulation that is turning hostile.

It is possible to turn back without losing the benefits. FHE allows the chain to keep offering loyalty programs, teleconsultation, personalized recommendations, pharma partnerships — **without ever seeing the individual customer**. It is possible to keep doing everything the chain needs to do. It is possible to do it while the chain keeps, with mathematical proof, that that customer was never exposed.

What is at stake is not a technical feature. It is the possibility for the chain to become again, unambiguously, what it has always claimed to be: a space where the customer is cared for, not surveilled.

> *“Within three years, some chain will lead. 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.

— End of Volume I

APPENDIX A

PT EN

Executive *Glossary*.

FHE

Cryptography that allows computing over encrypted data without decrypting it.

RLWE

Mathematical problem at the base of modern FHE.

CKKS, BFV/BGV, TFHE

The three main schemes in practical use.

PSI — PRIVATE SET INTERSECTION

Lets two chains discover shared customers without revealing entire bases. Central to fraud fighting.

RWE — REAL WORLD EVIDENCE

Clinical evidence derived from real-world usage data. A market dominated by IQVIA, with room for an FHE-based entrant.

NATIONAL DRUG TRACKING SYSTEM (SNGPC)

Brazilian system for managing controlled products (ANVISA).

LGPD ART. 11

Article classifying health as a special category of personal data.

CFF

Federal Pharmacy Council — regulator of pharmacist teleconsultation.

LATTIGO, OPENFHE, CONCRETE

Main FHE libraries.

PT EN

APPENDIX B

PT EN

Vendors and *Partners*.

VENDOR	FOCUS
Tune Insight	Lattigo, focus on health and clinical data
Owkin	FL+FHE for clinical research
Zama	Concrete, TFHE
Duality	OpenFHE, focus on health and finance
Inpher	Hybrid FHE+MPC
Stickybit	Brazilian technical boutique in FHE/PQC

APPENDIX C

PT EN

30 Questions for the *CDO/Commercial Director*.

Strategy

1. Who in our company understands advanced cryptography?
2. What is our current exposure to clinical-data processing?
3. How many external vendors have technical access to customer data?
4. Do we have an inventory of which data leaves the chain?
5. What is the current legal liability in sharing with pharma and health plans?

Priority use cases

6. How much is it worth to unlock selling RWE to pharma without risk?
7. How much do we lose each year to controlled-substance fraud?
8. What percentage of our chronic customers abandon treatment?
9. Which partnerships with operators are blocked today?
10. Which new app features were not launched due to privacy concerns?

Technical

11. Which FHE scheme for our first case?
12. Acceptable latency for our cases?
13. How do we integrate with POS, ERP, CRM, app?
14. How do we manage keys across chain, customer and partner?
15. Is threshold cryptography compatible with our flow?

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 compliance?
21. DPO engaged in the design?
22. Dialogue with the Brazilian Data Protection Authority (ANPD)?
23. Communication to the customer?

Commercial

24. Will pharma pay for FHE insights?
25. Will an operator accept cross-matching under cipher?
26. How do we price FHE-backed services?
27. Would other chains join an anti-fraud consortium?
28. How will we communicate publicly?
29. Internal case study to validate the thesis?
30. Worst-case scenario if a competitor announces first?

PT EN

The Counter That Does Not Remember

Strategic eBook for the senior leadership of large pharmacy chains.
Volume I · Edition 2026 · Confidential distribution.

Set in Iowan Old Style and SF Pro.

— end —