

STRATEGIC EBOOK · EXECUTIVE LEADERSHIP

---

FOR CEOS, CHIEF MEDICAL OFFICERS, CLINICAL DIRECTORS, CIOS,  
RESEARCH DIRECTORS AND BOARDS OF HOSPITALS AND HOSPITAL  
NETWORKS

# Trust That *Calculates.*

*How Fully Homomorphic Encryption allows hospitals to share knowledge without sharing patients, collaborate without ceding control, and participate in data-driven medicine without betraying the oath of confidentiality.*

---

VOLUME I · EDITION 2026 · CONFIDENTIAL

# What you will *read*.

*This eBook is a decision document. It was written to be read in a board meeting, on a trip between medical congresses, or on a Saturday morning before a long-term architecture decision.*

<b>00</b>	<b>Executive Summary</b>	<b>3</b>
	<i>The argument in one page</i>	
<b>I</b>	<b>The Hospital as Vault</b>	<b>5</b>
	<i>Why the hospital is today the most valuable and most paralyzed data asset in healthcare</i>	
<b>II</b>	<b>The Regulatory Tightening</b>	<b>9</b>
	<i>LGPD, HIPAA, GDPR, CNS, CFM—and the end of the era when medical records could be Excel files</i>	
<b>III</b>	<b>FHE in Executive Language</b>	<b>13</b>
	<i>What it is, without the math—and why it changes hospital economics</i>	
<b>IV</b>	<b>Use Cases by Area</b>	<b>17</b>
	<i>Multicentric research, radiological AI, tumor boards, benchmarking, telemedicine, value-based care, transplantation, teaching</i>	
<b>V</b>	<b>The Economics of the Sharing Hospital</b>	<b>29</b>
	<i>Real costs, ROI, and where returns emerge</i>	
<b>VI</b>	<b>Competitive Advantage and Institutional Reputation</b>	<b>35</b>
	<i>Why this is trust management, not IT</i>	

**VII** 24-Month Roadmap

*From board decision to first inter-institutional collaboration*

**PT** **EN**

---

**VIII** Risks, Mitigations, and Pitfalls

45

*What can go wrong and how to avoid it*

---

**IX** Manifesto

49

*A letter for the next decade of hospital care*

---

**·** Appendices

53

*Glossary, vendors, 30 questions for the CIO/Chief Medical Officer*

---

# The argument on *one* page.

*If you're only going to read one thing from this eBook, read this.*

**T**he modern hospital is, simultaneously, the most valuable data asset and the most paralyzed data asset in the entire healthcare chain. No other institution accumulates longitudinal medical records, medical imaging, anatomic pathology, genomic data, clinical evolution and patient outcomes the way a reference hospital does. And no other institution is able to do so little with that archive—because regulation, ethical responsibility and the oath of confidentiality that sustain the medical profession rightly prevent data from leaving the silo where it was generated.

The practical consequence is a structural contradiction. Elite hospitals have cohorts that could transform data-driven medicine—and cannot cross-reference them with other centers without months (sometimes years) of ethical and legal approval. Physicians have rare clinical cases that would benefit from international second opinions—and rely on de-identified emails in a fragile chain of custody. Researchers publish less than they could because every multicenter study is a marathon of DUAs (Data Use Agreements), renegotiated informed consents and parallel committees. Health plans want to cross-reference data for value-based contracting—and cannot do so without exposing the individual patient. AI vendors offer inference on medical imaging—and demand that the image be sent to a server no one at the hospital controls.

Each of these frustrations is real, well known, and has been addressed for the past fifteen years with the same answer: **more governance, more contracts, more committees, more auditing**. The answer has been marginally effective and structurally insufficient. Each new layer of governance adds cost and time without solving the central problem, which is the absence of a mathematical guarantee that individual data cannot be seen.

That guarantee now exists. It's called Fully Homomorphic Encryption—FHE. In one sentence: it allows two or more hospitals to compute jointly over their data without any of them seeing each other's data, and without any central server ever having the data in the clear. It is not a governance promise. It is a verifiable mathematical theorem.

1

SHARE WITHOUT EXPOSING

2

Five hospitals can run a joint study on ischemic stroke without any medical record leaving any of the centers.

## BENCHMARK WITHOUT PUBLIC RANKING

PT EN

Hospitals compare quality with each other without absolute numbers turning into negative PR for anyone.

## 3

### AI WITHOUT HANDING OVER THE PATIENT

Inference models on medical imaging run over an encrypted exam—the vendor never sees the patient.

## 4

### VERIFIABLE TRUST

The hospital can tell the patient, with mathematical proof: "your data never left us, even when we collaborated with others".

The thesis of this eBook is direct:

---

*“The next decade of hospital care will be defined by which institutions first learn to collaborate mathematically—preserving the oath of confidentiality while multiplying the scientific impact of what they know.”*

---

The computational cost of FHE is high, but decreasing, and—for reference hospitals—perfectly absorbable by the clinical IT budget. The cost of not acting is higher: it means remaining outside European consortia, outside elite collaborative studies, outside value-based care contracts, and increasingly surrounded by regulators. Institutions that move first will not merely gain capability—they will define the technical standard the others will have to follow.

The question for the board of any reference hospital is not "whether" to invest in private computing. It is "how can we lead this transition rather than be dragged along by it once regulators, patients and partners have already decided for us".

# The Hospital as *Vault*.

*The modern hospital is, without exaggeration, the richest health data vault on the planet—and the most underused. This contradiction is not a technical problem. It is a structural question about trust, responsibility and what it means to collaborate without betraying the patient.*

**T**hink about the archive a reference hospital accumulates in a single decade of operation. Hundreds of thousands of longitudinal medical records, with detailed clinical evolution of patients followed for years. Millions of images—X-rays, MRIs, CT scans, echocardiograms, mammograms, digital anatomic pathology. Laboratory results. History of medications administered, with time, dose and response. Adverse events, complications, readmissions. Biopsies stored in biobanks. In hospitals that have advanced into precision medicine, genomic sequences, transcriptomic profiles, microbiome data. Connected wearables, continuous monitoring data from ICUs. PROs, quality of life.

Each of these data points was born of a concrete clinical decision: this exam was ordered, this procedure was performed, this outcome was observed. The aggregate consequence is an archive whose scientific density is literally unprecedented in the history of medicine. A single reference hospital accumulates, in five years, more structured clinical data than all medical literature accumulated before the year 2000.

And almost none of it can be used outside the hospital itself without massive friction. This is the central contradiction of data-driven medicine in 2026: **never has there been so much material available, and never has it been so hard to take advantage of it.**

## Why this archive is paralyzed

It is not paralyzed for lack of technology, lack of scientific interest, or lack of demand. It is paralyzed for three structural reasons that reinforce one another:

### 1. THE OATH OF CONFIDENTIALITY

All of Western medicine is built on an ancient promise: what the physician sees and hears from the patient, he keeps. This promise is not a metaphor—it is the ethical foundation of the profession and

carries legal force in every jurisdiction in the world. Every time a hospital thinks about "sharing data", it is implicitly asking whether it is honoring or betraying that promise. The default answer has been maximum caution—and that caution is, in essence, correct.

## 2. LEGAL LIABILITY

A medical record leak creates civil, criminal and regulatory liability against the institution. The risk is asymmetric and brutal: the gain from sharing is diffuse (more science), the cost of a leak is concentrated (the institution that leaks pays). Legal departments and DPOs rightly operate under a logic of absolute risk minimization. The result is a system in which almost everything that could be collaborative ends up isolated.

## 3. THE OPERATIONAL COST OF CONTRACTUAL GOVERNANCE

When two hospitals decide to collaborate, even under legitimate structures (CEP/CONEP in Brazil, IRB in the U.S., European ethics committees), the approval time is measured in months, not weeks. DUAs must be negotiated. Informed consent forms must be revised or redrafted. Ethics committees at both centers must approve independently. The logistics of moving data between institutions are technically and legally complex. The result is that truly collaborative multicenter research—the kind that generates the most scientific value—is rare.

# The hospital's invisible assets

It is important to name what is at stake, because many people on hospital boards still think of "data" as an Excel file or a management system. What the hospital has today, and is not using, is much more than that:

ASSET	WHAT IT IS	WHY IT IS UNIQUE TO THE HOSPITAL
<b>Longitudinal cohort</b>	Patients followed for years with complete clinical evolution	No pharma sponsor has access to this follow-up; no claims data has this depth
<b>High-quality medical imaging</b>	Exams with standardized protocol and specialist report	The report is the asset, not the image; only the hospital has the image+report pair
<b>Digital anatomic pathology</b>	Histology slides scanned in high resolution	The physical biobank is at the hospital; the digital counterpart is too
<b>Real adverse events</b>	Complications observed in real time, with context	Public pharmacovigilance under-reports; the hospital knows what happened
<b>Physician behavior</b>	Prescribing patterns, procedure choice, success rate	Material for quality benchmarking, with no public parallel
<b>Severity-adjusted outcomes</b>	Mortality, readmission, complication adjusted by case-mix	Each hospital has its own, nobody shares for fear of PR fallout

## The historical parallel—and why hospitals are different

In other sectors, the transition from "silos" to "data collaboration" was forced by entrants that commoditized the infrastructure. Banks went through it with fintechs. Media went through it with platforms. In hospital healthcare this has not yet happened—not because the industry is immune, but because ethical and regulatory barriers slowed the cycle. That window of protection is closing.

The difference that matters, and that should guide hospital strategy, is that **the hospital has a unique structural advantage: patient trust**. Patients trust their hospital in a way they trust no other institution in the healthcare chain. This trust is the sector's most durable asset. Sharing data irresponsibly is the fastest way to burn this capital. Sharing data in a mathematically verifiable way is the most elegant way to multiply it.

*“The hospital that learns to collaborate without exposing is not losing control. It is discovering what it always knew: that the oath of confidentiality and participation in science can coexist—now with mathematical proof.”*

---

# The Regulatory *Tightening*.

*Hospital data regulation was, until five years ago, loose, regional and tolerant. It no longer is. And in the next three years it will become the central vector of pressure on hospital operations.*

There is a comfortable and mistaken perception shared by much of hospital leadership: that current health data regulation, although heavy, can be managed with a well-drafted consent form, a well-communicated privacy policy, and a dedicated DPO. This view works in 2024. It does not work in 2027. And hospitals that accept it as truth will be caught off guard by changes already underway that have not yet been fully felt.

## LGPD and article 11—health as a special category

The LGPD (Brazilian data protection law) places health data in the most protected category. Article 11 requires specific and robust legal grounds for any processing, and exceptions for "health protection" are interpreted narrowly. The Brazilian Data Protection Authority (ANPD) has not yet tested these limits at large private hospitals, but the signal is clear: **it is coming**. In 2025 the authority opened the first formal investigation against a large healthcare provider for sharing data with third parties without demonstrable legal grounds. It will be the first of many.

The detail that few Brazilian hospitals have internalized: the hospital's responsibility for the data **does not end when it shares it with a supplier**. If the AI vendor, the telemedicine system, or the health plan leaks the data, the hospital is jointly liable. The entire chain of hospital technology suppliers has become, in five years, a source of systemic risk.

## HIPAA and the obsolescence of anonymization

Hospitals operating in the United States have lived under HIPAA for decades. The central defense historically has been "Safe Harbor de-identification"—removal of the 18 identifiers. This defense worked in a world where re-identification required substantial effort. That world is over. Several studies

published in recent years have demonstrated re-identification of "HIPAA-compliant data" at rates above 80% using quasi-identifier attributes cross-referenced with public bases (voter rolls, ZIP lists, social profiles).

HHS has already opened multiple investigations against medical centers for use of "anonymized data" that was re-identified. The defense of "we removed the 18 identifiers" is no longer a defense—it is evidence that someone tried to minimize without understanding the current problem.

## GDPR and the European EHDS

GDPR is more aggressive. European hospitals already face dozens of fines per year for fragile legal grounds in data sharing, international transfer without safeguards, and processing of sensitive data without robust consent. The instrument that will redefine all of this is the EHDS—European Health Data Space—which takes effect in phases through 2027.

EHDS matters for Brazilian hospitals not because it will be applied here, but because it creates **the technical standard that regulators worldwide will adopt**. Within three years, any hospital that wants to participate in European multicenter research, or to be cited as an international reference, will need to demonstrate privacy-preserving analytics capability. Those who don't will be excluded for technical incapacity—not for bad faith.

## CFM, CNS and the specific Brazilian risk

In Brazil there is an additional layer: resolutions from the Federal Council of Medicine (CFM) on electronic medical records, telemedicine and use of AI in medical acts. The CFM has moved with surprising speed over the past three years, publishing resolutions that establish increasingly specific technical and ethical requirements. The CFM resolution on AI in diagnosis, in force since 2023, requires decision traceability and process transparency—requirements that traditional systems struggle to meet.

In parallel, the National Health Council (CNS) has been revising clinical research rules, and the Research Ethics Committee (CEP/CONEP) has tightened its interpretation of "secondary use of data" for research. Each of these changes, in isolation, looks technical. Combined, they form a gradual tightening that makes traditional operations increasingly fragile.

# The conceptual shift: proven, not declared, minimization

PT EN

All regulation is converging toward a single principle:

---

*“Having a policy is not enough. You need technical proof that the data could not have been handled any other way.”*

---

It is precisely at this point that FHE stops being a technical curiosity and becomes a regulatory defense tool. A hospital that processes data under FHE can demonstrate to ANPD, to HHS, to CNIL, or to its own ethics committee that individual data was never accessible, even during collaboration with other institutions. This is not a policy. It is a theorem verifiable by a third party.

# The cost of inaction, in numbers

PT EN

RISK	5-YEAR PROBABILITY	TYPICAL IMPACT
LGPD fine for sharing without robust legal grounds	High in Brazil	2% of revenue or R\$ 50M, whichever is greater
ANPD investigation for supplier-side protection failure	Medium-high	Reputation + costly remediation obligation
Class action over medical record leak	Medium	R\$ 100M+ in large breach cases
Exclusion from European consortia for technical incapacity	High	Loss of access to cohorts and international funding
Loss of research contracts with global pharma	Medium-high	R\$ 5M–50M annually per contract
Reputational crisis after public breach	Low-medium	18-36 months of drop in private occupancy

## THE STRATEGIC WINDOW

Regulators are looking for exemplary cases to cite in guidelines. The first Brazilian reference hospital to present an auditable FHE architecture becomes an official citation—regulatory protection + sector positioning in a single move.

# FHE in Executive *Language*.

*No math. No jargon. Only what the board needs to understand in order to make a long-term decision.*

Imagine a transparent vault. You can see that there is something inside, but you cannot see what it is. Now imagine that, from outside the vault, with mathematical gloves, you can manipulate the contents: add two things that are in there, multiply, compare, compute regressions, train models. You execute operations on the contents of the vault without ever opening it. When you finish, you return the closed vault to the key holder, who opens it and sees the result. This is FHE, in one sentence.

## The conceptual leap

All the cryptography your hospital uses today—TLS on the patient portal, AES on medical record backups, HTTPS on APIs—protects data in *two* of the three possible states:

- **In transit**—between devices. Solved by TLS.
- **At rest**—stored. Solved by AES.
- **In use**—when the server processes it. *Here the data has to be in the clear.*

The third state is the Achilles' heel of every hospital privacy architecture in history. When the medical record system runs a query, it *has to* see the data in the clear. When the AI vendor runs inference on an MRI, it *has to* see the image. When two hospitals collaborate on a study, someone *has to* see both sets of data. That is the moment the data is vulnerable to a dishonest employee, to intrusion, to a misconfigured backup, to a log retained for years, to a careless supplier, to a fragile integration between legacy systems.

FHE eliminates the third state. The server processes the data **without ever having access to the plaintext**. This is a phase change, not an incremental improvement.

## ANALOGY

The hospital "locks" its patients' data in a mathematical box using a key that only it holds. It sends the closed box to a neutral server (it could be cloud, a partner, a multi-hospital consortium). That server—which *never* receives the key—performs all desired computation *on the closed box*. The result is a new box, still closed, returned to the hospital. Only the hospital, with its key, opens the result. At no point in the chain has the server (or another hospital, or the AI vendor) seen the patients' data.

## What FHE offers that nothing else does

TECHNOLOGY	WHAT IT PROMISES	WHERE IT FAILS
HIPAA / LGPD anonymization	"We removed identifiers"	Trivial re-identification via cross-referencing; already invalidated
TEE (hardware enclave)	"The chip isolates"	Trusts the manufacturer; several side-channel attacks published
Federated Learning	"Data stays at the hospital"	Gradients leak data; already demonstrated in clinical research
Differential Privacy	"We add noise"	Good for aggregate statistics, bad for individual clinical decisions
Synthetic Data	"Artificially generated data"	Doesn't capture the long tail; doesn't replace real data
<b>FHE</b>	<b>"Server never sees plaintext"</b>	<b>High computational cost—but decreasing</b>

FHE is the only technology on this list whose guarantee is **mathematical and auditable by a third party**. For a regulator, for an ethics committee, for a distrustful patient, for a cautious legal counsel, the difference between "believing in governance" and "verifying mathematically".

## The three flavors that matter for a hospital

### CKKS

ML, STATISTICS, IMAGING

For cohort statistical analysis, AI training and inference, medical imaging processing.  
Implemented by Lattigo and OpenFHE.

### BFV/BGV

CLINICAL DATABASE

For exact queries over encrypted medical records, counts, stratification. When the result must be identical to plaintext.

### TFHE

LOGICAL DECISIONS

For eligibility algorithms, rule-based clinical decisions, fine-grained comparisons. The most flexible of the three.

### Hybrid

WHAT WORKS IN PRACTICE

Real systems combine two or three.  
Radiology inference in CKKS, queries in BFV, eligibility in TFHE.

## The cost myth: what you need to know

The standard argument against FHE is "it's too expensive". For hospitals, this is a half-truth that needs to be dismantled:

- **Cost has dropped two to three orders of magnitude** in seven years. The curve is steady.
- **For most hospital use cases** (cohort statistics, inference on a single exam, medical record queries), latency today is seconds to minutes—perfectly compatible with non-emergency clinical workflow.
- **Hardware accelerators** are reaching the market and promise another 10–100× in the next 24 months.

- **The right model is selective:** use FHE at the sensitive core (inter-institutional cross-referencing, AI inference on exams, data aggregation for benchmarking) and keep the rest of the operation local and clear. This cuts total cost to a fraction of a hospital's current IT budget.

For a reference hospital with annual revenue above R\$ 1 billion, the total investment in FHE—initial capex plus annual opex—comes in below 0.5% of the IT budget. It is less than many hospitals spend on a single upgrade of the electronic medical record system.

# Use Cases by *Area*.

*What concretely changes in each area of hospital operations. Research, radiology AI, tumor boards, benchmarking, telemedicine, value-based care, transplantation, teaching—each with its own specific opportunity.*

## Collaborative multicenter research

This is the area where FHE has the most immediate and most transformative impact for reference hospitals. Multicenter research is the only way to generate robust evidence in rare diseases, specific populations, and outcomes that require large cohorts. Today, this kind of research faces approval timelines measured in years.

### 1. OBSERVATIONAL STUDIES ACROSS FIVE OR MORE CENTERS

In the traditional model: each center contributes anonymized data, aggregated on a central server, with DUAs negotiated bilaterally, independent ethics committees, harmonized consent forms. Average timeline: 18–24 months from the start of the conversation to the first data available for analysis. With FHE: each center keeps data local, encrypts with the consortium key, contributes only encrypted statistics. The aggregator computes means, regressions, survival, predictive models over the ciphertexts. Average timeline: 6–9 months to first analysis. A 60% reduction in time, with ethical governance that is **more robust**, not less.

### 2. RARE DISEASES

In rare disease, no single hospital has a cohort sufficient for meaningful study. The solution is to cross bases. The traditional solution does not work because each patient is potentially identifiable by rare characteristics. FHE solves it: hospitals contribute encrypted data, analysis happens under encryption, the result is aggregate statistics that do not allow re-identification. **Rare diseases become studyable at scale.**

### 3. INVESTIGATOR-INITIATED STUDIES

The hospital's physician-researcher wants to test a clinical hypothesis that requires data from other centers. Today this is practically unfeasible outside of formal consortia. With FHE, the investigator can

propose collaborative studies to colleagues without having to go through the entire institutional DUA and contractual governance apparatus—because technical collaboration resolves most legal concerns

PT EN

## AI applied to medical imaging

AI vendors for radiology, anatomic pathology, ophthalmology and dermatoscopy offer increasingly useful models. But all of these models require the image to be sent to the vendor's server. This creates a chronic problem: the hospital is caught between the desire to offer the best care (which includes AI) and the obligation to protect the patient's image.

### 1. DIAGNOSTIC INFERENCE WITHOUT SENDING THE IMAGE TO THE VENDOR

With the right architecture, the hospital can use the vendor's model without ever sending the image in the clear. An extraction CNN (ResNet-50 or equivalent) runs *locally at the hospital*, in the clear, over the image. It produces a 2,048-dimensional embedding that captures all diagnostically relevant information. Only the embedding is encrypted and sent to the vendor. The vendor runs the final linear classifier under FHE and returns the encrypted score. **The vendor never sees the image or the embedding in the clear—it is the pattern used by Owkin in partnerships with international oncology centers.** The patient never leaves the hospital's control. The hospital gains the benefit of AI without the legal liability of biometric data transfer.

### 2. FEDERATED TRAINING WITH ENCRYPTED GRADIENT AGGREGATION

Multiple hospitals want to train a collective model (sepsis prediction, post-surgical complication, readmission). Each hospital trains locally on its own patients—without moving data. The gradients resulting from training are *encrypted* before leaving the hospital. A neutral aggregator sums the gradients under encryption (federated average) and returns the encrypted mean gradient. Each hospital applies the gradient to the local model. This pattern (FL + FHE) corrects the gradient leakage that pure FL has—research has already shown that patient data can be reconstructed from plaintext gradients.

**Encrypted aggregation makes FL defensible for clinical data.**

### 3. EXTERNAL VALIDATION OF AN INTERNALLY DEVELOPED MODEL

The hospital developed a model to predict post-surgical complications. To publish, it needs to validate the model on an external cohort. The partner hospital agrees, but requires that its data never be exposed. FHE allows validation under encryption: hospital A's model runs on hospital B's encrypted data, and the performance metric is computed without either side seeing what belongs to the other.

# Tumor boards and second opinions

PT EN

Multidisciplinary tumor boards and international second-opinion requests are part of the daily life of reference oncology hospitals. Today they run on email, with de-identified images exchanged as PDFs, in a fragile chain of custody. For VIP cases, with expectations of absolute confidentiality, the friction is constant.

## 1. INTERNATIONAL TUMOR BOARD UNDER ENCRYPTION

Four oncologists in four countries discuss a complex case. Each one annotates observations on the encrypted case. The system aggregates annotations without anyone seeing the patient's name. Applicable both to individual cases (high complexity, low frequency) and to recurring cohorts (study of rare subgroups).

## 2. REMOTE SECOND OPINION WITHOUT IMAGE TRANSFER

A small hospital requests a second opinion from a reference center. The image is encrypted, sent encrypted, and the reference center's specialist runs analysis under encryption (with expertise encoded in models), returning an encrypted report. **The reference center never archives the original image—it cannot.** This drastically reduces the reference center's legal liability and dramatically expands the number of second opinions it can offer.

# Quality benchmarking among hospitals

This is a case that deserves special attention because it is where FHE unlocks something that *no other solution* can unlock. Hospitals want to compare quality with one another—adjusted mortality rate, 30-day readmission, length of stay, surgical complications. The scientific and operational benefit of the benchmark is enormous. The obstacle is simple: **no hospital wants absolute numbers to turn into negative PR.**

FHE solves it: each hospital encrypts its quality data. The aggregator computes percentiles and returns to each hospital its relative position, **without any hospital seeing the absolute numbers of the others.** Hospital A discovers it is at the 75th percentile in adjusted mortality for myocardial infarction, without knowing which hospital sits at the 90th percentile. The entire public conversation about hospital quality changes—for the first time there is a reliable sector benchmark that does not create exposed losers.

This is particularly important in Brazil, where current benchmarks (ONA, JCI) are structurally unable to offer this kind of comparison. The first consortium of Brazilian hospitals to adopt FHE for benchmarking will redesign the sector's conversation about quality.

## 1. INTER-INSTITUTIONAL TELEMEDICINE WITH REAL PROTECTION

A patient from hospital A has a consultation with a specialist at hospital B via telemedicine. Today, that means hospital B's system must receive the patient's medical record. With FHE, the specialist sees only what is necessary for the consultation, and no persistent copy of the record is created at hospital B.

## 2. CONTINUOUS MONITORING WEARABLES

Patients with chronic disease use wearables that send continuous data to the hospital. This data is highly identifiable and highly sensitive. Under FHE, monitoring (event detection, deterioration alerts, medication adjustment) happens over encrypted data. The hospital intervenes when needed, without maintaining a continuous individual database in the clear.

## Value-based care and payer contracts

Outcome-based contracts are the trend of the decade. They require continuous cross-referencing among dispensing (payer), utilization (hospital) and clinical outcomes. Today this cross-reference is war—audits, denials, conflict. With FHE, both sides can compute on the cross-reference without exposing each other's base. Result: less friction, fewer legal disputes, outcome-based contracts that actually work.

## Organ transplantation

Transplant systems require cross-referencing potential recipients with available donors, with complex immunological matching. The data involved is highly sensitive, and the logistics are national or international. FHE allows matching to happen on encrypted data, with the decryption key distributed among the national center, origin hospital and recipient hospital—no single party can see data it shouldn't.

## Teaching, residency and student research

Residents and medical students need exposure to real cases in order to learn. Today, this means direct access to the medical record—with all the governance fragility that implies. Under FHE, it is possible to build teaching environments where the case is presented without exposing identifiers, and where the

student interacts with encrypted versions in a controlled way. Teaching with data protection stops being an oxymoron.

PT

EN

# The Economics of the *Sharing Hospital*.

*The real numbers. How much it costs, how much it returns, and where hospital operations find the value.*

Every investment decision in a hospital boardroom has to pass through three sieves: capex, recurring opex, and impact on operational and scientific metrics. FHE is no exception. The calculation, for a reference hospital with annual revenue between R\$ 500M and R\$ 5B, is more favorable than it appears at first glance—because the downside is budgetable and the upside is structurally asymmetric.

# The cost of doing it (initial capex)

PT EN

COMPONENT	TYPICAL INVESTMENT
Founding team (1 senior crypto engineer, 2 ML engineers, 1 clinical PM, 1 privacy counsel)	R\$ 4M – 6M / year
Licenses and tooling (Lattigo open, Concrete, OpenFHE)	R\$ 200k – 800k / year
Infra: GPUs and CPUs with AVX-512 acceleration	R\$ 1.5M – 3M initial
Strategic consulting (Tune Insight, Owkin, Duality)	R\$ 800k – 2M
Regulatory study with a healthcare-specialized firm	R\$ 400k – 1M
Integration with existing systems (EMR, PACS, LIS)	R\$ 800k – 2.5M
<b>Year 1 total</b>	<b>R\$ 8M – 15M</b>

# The cost of running it (recurring annual opex)

ITEM	ANNUAL ESTIMATE
Compute (FHE 100x–1000x more expensive than plaintext in the sensitive core)	R\$ 2M – 6M
Maintenance team (4–6 engineers + 1 legal advisor)	R\$ 4M – 7M
Annual security audit	R\$ 500k – 1.5M
<b>Stabilized annual opex</b>	<b>R\$ 6.5M – 14.5M</b>

For a hospital with revenue above R\$ 1B, this represents between **0.5% and 1% of revenue**. It is comparable to the cost of maintaining a realistic simulation center, or to the cost of a single ICU renovation. For reference hospitals with revenue above R\$ 3B, it is a rounding error in the budget.

PT EN

## The return—where the money reappears

FHE ROI in hospitals comes from six vectors that must be modeled separately. Unlike cosmetics or pharma, in hospitals most of the return is not new revenue—it is loss avoidance, enablement of new capabilities, and appreciation of a long-term asset (institutional reputation).

### 1. Research revenue and participation in clinical trials

Reference hospitals generate significant revenue as investigator sites in pharmaceutical industry clinical trials. Each new phase III trial can bring R\$ 2M–10M to the hospital. Hospitals with FHE capability become preferred partners for sensitive trials (decentralized, international multicenter, studies involving genomic data). Estimate: **3–8 additional trials per year**, generating R\$ 10M–60M in incremental annual revenue.

### 2. Enablement of value-based care contracts

Payers are pushing for outcome-based contracts. Hospitals that can operate this model with robust data governance capture premium contracts. Estimate: **2–4 additional VBC contracts** over 36 months, with annual value of R\$ 5M–30M each.

### 3. Access to international consortia and research funding

Elite Brazilian hospitals today receive between R\$ 5M and R\$ 50M annually in international research funding (NIH, Wellcome Trust, Horizon Europe, private foundations). FHE enables participation in consortia that today require technical capability few have. Estimated increase: **30–60%** within three years.

### 4. Reduction of regulatory and legal risk

Expected exposure to LGPD fines, leak-related lawsuits, and post-incident remediation is estimated at R\$ 30M–150M of present value over 5 years for reference hospitals. FHE drastically reduces both probability and magnitude. Treated as a hedge: **R\$ 12M–60M in insurance value**.

## 5. Operational efficiency in research

PT EN

The average contractual governance cost per multicenter study is R\$ 200k–600k. A reference hospital typically runs 50–150 collaborative studies per year. Estimated reduction with FHE: **30–50% of governance cost**, or R\$ 3M–25M annually.

## 6. Institutional reputation and talent attraction

Hard to quantify but real. Hospitals recognized as "leaders in data governance" attract top physician-researchers, receive more invitations to elite collaborations, and capture positive media visibility. The present value of this is measurable only in retrospect, but sector analogies (hospitals that led on patient safety, humanization, sustainability) suggest impacts of **10-20% on institutional reputation metrics** over a 5-year horizon.

### The business case, summarized

~R\$ 11M

YEAR 1 INVESTMENT

~R\$ 10M

STABILIZED ANNUAL OPEX

R\$ 80M+

VALUE ENABLED OVER 5 YEARS

8x–15x

EXPECTED ROI OVER 5 YEARS

---

*“In any honest modeling, FHE for a reference hospital is the digital transformation investment with the greatest asymmetry of return available in 2026.”*

---

Not because high return is certain. But because the downside is trivially small (known cost, perfectly budgetable) and the upside combines regulatory hedge, scientific enablement, incremental revenue and reputational upside in a single move—each of which, on its own, would justify the investment.

# Competitive Advantage and *Institutional Reputation.*

*FHE in a hospital is not, first and foremost, an IT decision. It is a decision about how the institution wants to be perceived and in which league it wants to play.*

**T**here is an important difference between the FHE thesis for hospitals and the thesis for other sectors. In cosmetics, FHE is brand narrative. In pharma, it is regulatory and scientific advantage. In hospitals, FHE is primarily **reputational capital and institutional positioning**. The hospital does not sell creams. It does not submit drugs to the FDA. The hospital sells, ultimately, trust—and trust is the hardest asset to build and the most fragile to maintain.

## What reputation means in a hospital

Hospital reputation is multi-dimensional: clinical quality, patient safety, medical excellence, hospitality, teaching, research. But there is a dimension that has remained invisible and will become central in the coming years: **trustworthiness in data handling**. Patients (especially premium patients who sustain margins) are starting to ask things they did not ask five years ago. "Do you share my data with the AI vendor?" "Do you let the medical record system access my psychiatric history?" "Are you participating in that genomics research consortium?"

Twenty years ago, these questions were unthinkable. Five years ago, they were rare. Today they are frequent. In three years, they will be the default. The question for the board is: is the institution ready to answer with mathematical truth, or only with institutional promise?

# The three possible positions

PT EN

## Position 1 – The Hospital That Leads on Trust

Focus on direct communication with the patient. A public program on how the hospital protects data. Annual external audit published. Explicit positioning as "the hospital you trust with your data". Works best for premium private hospitals (Einstein, Sírio, HCor, Oswaldo Cruz) where the premium patient is the direct customer and where institutional reputation is the core product.

## Position 2 – The Leading Academic Center

Focus on research and international collaborations. Positioned as the center technically and ethically capable of participating in the most sensitive consortia in the world. Attracts scientific talent, funding, partnerships with the global top 10. Works best for university hospitals and reference oncology centers.

## Position 3 – The Brazilian Sector Leader

Focus on building the sectoral FHE consortium. Leading the movement as "the hospital that organized private collaboration among Brazilian institutions". Captures the articulator role, gains institutional visibility, redesigns the public conversation about hospital quality. Works for any hospital with a C-level sponsor willing to invest political capital in the movement.

The three are not mutually exclusive. A robust strategy starts with one and expands to the others as capability matures.

## The difference for public hospitals

For Brazilian public hospitals (HC-USP, HC-Unicamp, HC-FMRP, INCA, HUPES, etc.), the calculation is different: competitive advantage is less relevant, but the scientific and regulatory advantage is even greater. A public reference hospital has unique cohorts (volume, population diversity, longitudinal follow-up under the Brazilian public health system (SUS)) that are a global scientific treasure. Today these cohorts are paralyzed by the same problems as private hospitals, plus the additional difficulty of public governance.

FHE for public hospitals is possibly the most transformative opportunity of the decade for Brazilian science. It allows HC-USP to collaborate with Karolinska without Brazilian patient data having to leave the HC's server. It allows INCA cohorts to be used in international oncology studies without violating

data sovereignty. It allows SUS—historically a pioneer in public health—to become a pioneer in data-driven private research.

PT EN

## The cost of not positioning

There is a scenario that must be made explicit in the boardroom: what happens if none of Brazil's reference hospitals adopt FHE structurally in the next 36 months?

Answer: **European and American hospitals will.** They will capture the position of "capable technical partner" in every international consortium. Brazilian hospitals will be progressively excluded from elite collaborations, not for lack of clinical quality, but for technical incapacity to participate under the new rules. Within five years, the gap will be structural and expensive to reverse.

---

*“A hospital that leads in FHE is not building IT capability. It is protecting its place among the centers that will still matter a decade from now.”*

---

# 24-Month *Roadmap*.

*From board decision to first inter-institutional collaboration. Four phases, clear milestones, exit metrics for each.*

## 01

MONTHS 1-6 · LEARN

### **Foundation and internal capability**

Hire the founding senior crypto engineer. This hire is the real bottleneck. For hospitals, the fastest path is often a partnership with a university that has the talent (USP, Unicamp, EPFL via a bridge with Tune Insight) while funding the applied team internally. In parallel: engage strategic consulting for the initial architecture, map three candidate use cases, align with the Research Ethics Committee (CEP/CONEP) and institutional legal.

**Exit metric:** documented technical architecture, three selected cases (ideally one internal research case, one radiology AI case, and one inter-institutional benchmark), favorable opinion from the institutional CEP.

## 02

MONTHS 7-14 · BUILD

### **Internal pilot in a controlled environment**

Build a single use case, end to end, in a controlled internal environment. Recommendation for hospitals: encrypted statistical analysis over the hospital's own internal cohort, without involving other centers yet. This validates the technology, trains the team, and produces the first defensible demo for the CEP, board, and external partners.

Validate latency, cost, accuracy, integration with existing systems (electronic medical record, PACS, LIS). In parallel: begin structuring materials for dialogue with partner hospitals and regulators.

**Exit metric:** functional demo on a real internal cohort, validated metrics, technical documentation ready to present to an external partner.

PT EN

## 03

MONTHS 15–20 · FIRST COLLABORATION

### **Joint study with at least one partner hospital**

Launch the first inter-institutional collaboration using the architecture. Suggestion: begin with a single trusted partner—preferably another reference hospital, Brazilian or international, with whom there is already a history of traditional collaboration. Ideal use case: an observational study on a well-characterized clinical outcome (post-surgical survival, complication rate for a specific procedure, treatment response).

Document everything. Iterate the architecture. Measure time-to-first-analysis versus the traditional model. Present the case at a congress (DIA, ASCO, Riamb, SBPC, SBC, etc.) as a reference.

**Exit metric:** first collaborative study completed under FHE, favorable opinion from both CEPs, first scientific publication in a high-impact journal.

## 04

MONTHS 21–24 · INSTITUTIONAL CAPABILITY

### **Adoption as a cross-cutting capability**

Make the architecture available to multiple internal and external programs. Train medical and research teams on how to propose studies under FHE. Launch the formal multi-hospital consortium (3–5 hospitals) on the infrastructure. Publish a technical whitepaper. Present in regulatory forums (ANPD, CEP/CONEP). Position publicly.

This is the phase in which the investment of the previous 20 months begins to generate return at scale. Done correctly, it produces sustained sector recognition and a preferred position in future collaborations.

**Exit metric:** 5+ internal programs using the capability, formalized multi-hospital consortium, first mention in a public guideline from ANPD or a medical society.

# Milestones the board should demand

PT EN

MILESTONE	WHEN	WHY IT MATTERS
Founding crypto engineer hired or university partnership formalized	Month 4	Without this, there is no project
Use case selected and validated by the CEP	Month 6	Without ethical alignment, the project dies early
Technical demo on a real internal cohort	Month 14	Board-defensible proof of feasibility
First external collaboration initiated	Month 18	Institutional validation that the technology works in the real world
First scientific publication using the architecture	Month 22	Signal that the investment converts into academic reputation

# Risks, Mitigations and *Pitfalls*.

*What can go wrong, in decreasing order of probability and severity.*

## **Risk 1 · Internal cultural resistance**

**Probability:** high. **Impact:** manageable but persistent.

The biggest obstacle to FHE in hospitals is neither technical nor regulatory—it is cultural. Physicians and researchers are deeply cautious about technical novelty in clinical workflow. Legal departments and CEPs operate under absolute risk minimization logic. Every new actor in the project will rightly ask, "why change what works?"

**Mitigation:** treat it as a cultural project before a technical project. Engage medical and ethical champions from the start. Begin with low-risk, high-demonstration-value cases. Communicate internally in medical language, not IT language. Invite the CEP to co-design the technical governance.

## **Risk 2 · Inability to hire technical talent**

**Probability:** high. **Impact:** blocking.

Global FHE talent is scarce, and almost none of these professionals has ever considered working for a hospital. Compensation packages, cultural environment, and career profile are often incompatible with the expectations of a crypto researcher.

**Mitigation:** university partnership or talent acquisition via specialized consulting (Tune Insight, Owkin, Stickybit) is often more viable than direct hiring. The hospital does not need to have the talent in-house from day one—it needs to have the talent *available*.

## **Risk 3 · Integration with legacy systems**

**Probability:** high. **Impact:** manageable but expensive.

A typical reference hospital operates 30–80 distinct systems (EMR, PACS, LIS, RIS, ERP, departmental systems). Integrating FHE with that legacy stack is technically non-trivial.

**Mitigation:** don't try to integrate everything. Identify the 2–3 systems that matter for the first use cases (typically: EMR, PACS, research base). Build specific bridges. The rest of the legacy remains untouched.

PT EN

## Risk 4 · CEP or legal department blocking progress

**Probability:** medium. **Impact:** temporarily blocking.

CEPs and legal teams operate under conservative logic. A proposal that is too innovative may be rejected out of excess caution.

**Mitigation:** co-design with the CEP and legal from the start. Present FHE as a tool that strengthens the CEP, not a bypass. Bring in external opinions from already recognized institutions. Start with the easiest case to defend.

## Risk 5 · Computational cost not falling at the expected pace

**Probability:** medium. **Impact:** manageable.

For very high-volume cases (queries across the hospital's entire medical record, training on millions of images), the cost of FHE in 2026 is still challenging.

**Mitigation:** start with low-volume, high-value cases. Don't try to replace the whole infrastructure—only the areas where FHE makes a real difference.

## Risk 6 · A competitor announces first

**Probability:** medium. **Impact:** high for reputation.

Other reference hospitals may have parallel projects underway. Unlikely to be further along, but possible.

**Mitigation:** speed. Every month of delay is a month of risk. If a competitor does announce first, redirect the narrative to a specific niche (academic consortium, technical positioning, clinical specialty).

## Pitfall 1 · Treating it as an IT project

The most common mistake is placing FHE under the CIO rather than the Chief Medical Officer or Research Director. Result: perfect technical delivery and zero institutional impact. **FHE in a hospital should report to the Chief Medical Officer or the Research Director, with sponsorship from the CEO/Superintendent.**

## Pitfall 2 · Starting with the most ambitious case

PT EN

The temptation is to begin with the highest-impact case—often an inter-institutional benchmark or an international collaboration. It is a mistake. Ambitious cases require political coordination that takes time. Start internally, validate, and only then expand.

## Pitfall 3 · Forgetting key governance

FHE protects during computation. But key management is where most implementations fail. For hospitals, the right structure involves keys distributed among the institution, the CEP and an independent partner. **Key governance design is half the project.**

## Pitfall 4 · Underestimating ethical approval timelines

The institutional CEP may take 3–6 months to understand and approve a new proposal. Plan around that. Don't try to rush the CEP—that destroys the relationship. Educate it, yes, over time, with institutional patience.

# A letter for the next decade of *hospital care.*

*For the Superintendents, Chief Medical Officers, Research Directors,  
Board Members and CEOs of hospitals that can still choose to lead.*

**T**he institution you lead was built on an ancient promise, possibly the oldest of all professions: that there exists a space, in the midst of illness, where the patient can at the same time be rescued and respected. Where what they share in a moment of fragility is kept safe. Where trust is part of the treatment, not an add-on to the treatment. This promise has crossed centuries. It survived wars, epidemics, technological transformations, medical paradigm shifts. It survived because it was—and largely still is—true. People who choose to be treated at a reference institution trust it, deeply, with what is most intimate to them: their body, their clinical history, their vulnerabilities.

This promise, for centuries, was kept with simple instruments. The physician who guards. The sealed envelope. The locked archive. Discretion among peers. The oath of confidentiality was operational because clinical data was scarce, physical and local. It literally fit in a folder. Anyone who needed access had to be physically present.

But over the past twenty years, without anyone decreeing it, the environment in which this promise must be kept has changed completely. Clinical data is no longer scarce, physical and local. It has become abundant, digital and distributed. Every reference hospital today operates hundreds of systems, dozens of suppliers, cloud integrations, AI vendors, payer systems, telemedicine platforms, connected devices. Each of these is a place where data can exist in the clear. Each is a point where the ancient promise of confidentiality can fail—not through the hospital's bad faith, but because of the distributed, technical nature of the modern environment.

The result is an uncomfortable situation. Hospitals uphold the promise with the best of intentions, with growing governance, with investment in security, with competent DPOs. And even so, the structural base of the commitment is more fragile than it was in the last century. Not because hospitals are worse—but because the environment is more hostile, more interconnected, more distributed, more dependent on supplier chains no one fully controls.

It is possible to return to a robust form of keeping the ancient promise, without losing the benefits of the modern environment. FHE—Fully Homomorphic Encryption—is the first technology in decades that

makes this possible. It is possible to keep using AI to improve diagnosis, keep collaborating with other hospitals to do science, keep participating in research, keep offering telemedicine, keep processing data at scale. **It is possible to do all of this while the institution maintains, with verifiable mathematical proof, that the individual patient was never exposed.**

This sentence seems, on a first reading, paradoxical. On a second reading, it seems too technical. On a third, it seems like exactly what the medical profession has always tried to do—now finally with an instrument equal to the challenge. How is it possible to collaborate without exposing? Mathematics answers, and the answer is elegant, old, and at last viable in production.

What is at stake is not a technical feature. It is the possibility of a hospital institution becoming again, unambiguously, what it has always said it was: a space of trust where scientific collaboration and respect for the patient coexist without betraying either. Where "sharing knowledge" and "protecting the patient" cease to be goals in tension and become two dimensions of the same work.

This possibility is open today for a small number of Brazilian institutions. The first ones to understand what is in their hands. The first to make the right hire, call the right legal counsel, bring the case to the right board. The first to co-design the architecture with the CEP, the first to publish the first collaboration, the first to defend the position at a congress, in an interview, in an article, for two years in a row without giving in to the temptation to dilute the message.

Within three years, this position will be taken. Some hospital—Brazilian or international—will lead. The question for each institution's board is simple:

---

*“Will we be the hospital that showed the sector how it's done, or the hospital that had to learn later from whoever moved first?”*

---

There is a window. It is short. It is real. It is historically rare. Reference hospitals have, in prior decades, passed through similar windows—the transition to humanization, the transition to international accreditation, the transition to evidence-based medicine, the transition to patient safety. In each one, some hospitals led and others followed. Those who led captured reputational capital that sustains advantages to this day. Those who followed paid the cost of late implementation without any of the rewards.

This is the next window. It is possibly the most important of the decade, because it is the first in which the institution can choose to lead before being pressured—because the regulatory problem is still forming, because premium patient expectations are still forming, but the technical solution already exists and is ready to be adopted by whoever has the courage.

Whoever reads this eBook has a map in their hands. The map is not complete, not without risks, not without costs. But it is clear. And it is, at this moment, in front of the right people to make the right decision.

The rest is courage.

— *End of Volume I*

# Executive *Glossary*.

*The terms you will hear from the CIO, the Research Director, and the Research Ethics Committee (CEP/CONEP). In plain English.*

## **FHE — FULLY HOMOMORPHIC ENCRYPTION**

Encryption that allows computations to be performed on encrypted data without decrypting it. The result, when decrypted, equals what would have been obtained on the original data.

## **RLWE — RING LEARNING WITH ERRORS**

The mathematical problem on which most modern FHE schemes are based. It is the same problem underpinning the post-quantum cryptography standardized by NIST. Resistant to classical and quantum computers.

## **CKKS, BFV/BGV, TFHE**

The main FHE schemes in practical use. CKKS for ML and statistics; BFV/BGV for exact integers; TFHE for flexible Boolean logic.

## **CEP — RESEARCH ETHICS COMMITTEE**

The institutional body that approves research projects involving human subjects. In Brazil, regulated by the National Health Council (CNS). The CEP is the central ally of any hospital FHE project—not an obstacle.

## **CONEP — NATIONAL RESEARCH ETHICS COMMISSION**

National body that regulates clinical research in Brazil, under the Ministry of Health. Approves multicenter projects and studies in special thematic areas.

## **DUA — DATA USE AGREEMENT**

Bilateral contract between institutions defining how data can be used in a collaborative project. Traditional DUAs take months to years to negotiate. FHE dramatically reduces the complexity of that negotiation.

## **PACS, RIS, LIS**

PT EN

Picture Archiving and Communication System (medical imaging), Radiology Information System, Laboratory Information System. The main legacy systems with which FHE must integrate in a hospital.

## **EHDS — EUROPEAN HEALTH DATA SPACE**

European initiative creating common infrastructure for secondary use of clinical data in research. Defines the technical standard global regulation will adopt in the coming years.

## **THRESHOLD CRYPTOGRAPHY**

Technique that distributes a cryptographic key among multiple parties, requiring a quorum to use it. Essential for FHE architecture in a multi-hospital consortium.

## **PSI — PRIVATE SET INTERSECTION**

Protocol derived from FHE/MPC that lets two parties discover the intersection of their sets without revealing the rest. Useful for identifying patients common to multiple hospitals without exposing the bases.

## **FEDERATED LEARNING**

Distributed training where data stays local at each hospital. When combined with FHE for gradient aggregation (FL+FHE), it eliminates the leakage that pure FL suffers from.

## **LATTIGO, OPENFHE, CONCRETE**

Main FHE libraries in practical use. Lattigo (Go, Tune Insight); OpenFHE (C++, Duality); Concrete (Rust+Python, Zama).

# Vendors and *Partners*.

*Where commercial capability lives, where the talent is, and where active use cases already exist in hospital healthcare.*

## Specialized vendors and startups

VENDOR	HEADQUARTERS	FOCUS
<b>Owkin</b>	Paris / NY	FL+FHE for hospital research; partnerships with top oncology centers
<b>Tune Insight</b>	Switzerland (EPFL)	Lattigo; specific focus on multi-hospital federated medical research
<b>Zama</b>	Paris	TFHE, Concrete framework
<b>Duality Technologies</b>	USA / Israel	OpenFHE, focus on healthcare and finance, heavy consulting
<b>Inpher</b>	Switzerland / USA	Hybrid FHE + MPC, focus on healthcare
<b>Lifebit</b>	United Kingdom	Federated genomics platform for hospitals and biobanks
<b>Mozaic / TripleBlind</b>	USA	Privacy-preserving analytics for hospitals and payers
<b>Stickybit</b>	Brazil	Brazilian technical boutique in FHE/PQC; custom architecture

# Relevant initiatives and consortia

PT EN

- **Trustworthy Federated Data Analytics (TFDA)**—Helmholtz, Germany—privacy-preserving federated clinical research
- **NIH N3C**—National COVID Cohort Collaborative (applicable governance model)
- **European Health Data Space (EHDS)**—European infrastructure under construction
- **Global Alliance for Genomics and Health (GA4GH)**—standards for genomic data, including private computation
- **Federated Tumor Segmentation (FeTS)**—international consortium of oncology centers for federated AI
- **Swiss Personalized Health Network (SPHN)**—national model for federated clinical data governance

## Academic centers where the talent lives

- **EPFL (Lausanne)**—Christian Cachin, Jean-Pierre Hubaux, origin of Lattigo
- **USP / Unicamp / IME-USP**—advanced cryptography research with healthcare applications
- **IBM Research**—historical origin of FHE
- **Microsoft Research**—SEAL library
- **Université Paris-Saclay / ENS**—Léo Ducas, French crypto ecosystem
- **KU Leuven (COSIC)**—Frederik Vercauteren
- **Stanford / MIT / CMU**—several researchers active in clinical ML+FHE

# 30 Questions for the *CIO and Chief Medical Officer*.

*The list you should bring to the next joint meeting of your CIO, Chief Medical Officer and Research Director.*

## **Strategy and capability**

1. Do we have anyone on the team with a background in advanced cryptography? If not, what is the acquisition or partnership plan?
2. What is our current exposure to patient data processing, in volume and jurisdiction?
3. How many external vendors have technical access to our patient data today? In the clear or encrypted?
4. Do we have an up-to-date inventory of which data leaves the institution and where it goes?
5. What is our legal and CEP opinion on the sustainability of that architecture over the next 36 months?

## **Priority use cases**

6. Which internal research areas are most limited by the inability to cross-reference with other centers?
7. In which specialties do we have unique cohorts that would be worth sharing if we could?
8. Which AI vendors would we like to use but don't, out of fear of data exposure?
9. Which Brazilian or international hospitals would be natural partners for a first FHE collaboration?
10. In which clinical area would inter-hospital benchmarking have the greatest positive institutional impact?

## **Technical architecture**

11. Which FHE scheme makes the most sense for our first case? CKKS, BFV, TFHE?
12. Can we run basic statistical analysis on an internal cohort under FHE with acceptable latency today?

13. What is the estimated computational overhead for our priority use case?
14. How do we integrate with our existing systems (EMR, PACS, LIS, RIS)?
15. How do we manage keys among the institution, the CEP and external partners?
16. Who custodies the key in an international consortium?
17. Is our architecture compatible with threshold cryptography?

## Cost and infrastructure

18. Estimated computational cost per analysis, in FHE versus plaintext?
19. Which accelerators have we evaluated? FPGA? Specific GPU?
20. Will we build in-house, partner with a university, or use a vendor (Tune Insight, Owkin, Stickybit)?
21. What are the projected capex and opex over the next 24 months?
22. Do we have a confirmed C-level sponsor (CEO, Superintendent)?

## Ethics, regulation and compliance

23. Has the institutional CEP been formally engaged in designing the proposal?
24. Who will perform the independent security audit?
25. How do we demonstrate compliance with LGPD, HIPAA (if applicable), CNS?
26. Can we publish the architecture for public review?
27. Do we already have open dialogue with ANPD about the approach?
28. How do we communicate the initiative to patients and the public?

## Risks

29. Worst-case scenario if a competitor (another reference hospital) announces before us?
30. Worst-case scenario if the CEP or legal blocks progress?



## Trust That Calculates

Strategic eBook for executive leadership of hospitals and hospital networks.

Volume I · 2026 Edition · Confidential distribution.

Set in lowan Old Style and SF Pro.

Built as a self-contained HTML document.

Print on heavy stock for fidelity to the original layout.

— end —