

EBOOK ESTRATÉGICO · ALTA GESTÃO

PARA CEOS, CSOS, CMOS (CHIEF MEDICAL OFFICERS), HEADS OF R&D, CHIEF DATA OFFICERS E CONSELHOS DAS MAIORES FARMACÊUTICAS DO MUNDO

O Ensaio *Invisível*.

Como a Criptografia Totalmente Homomórfica redefine pesquisa clínica, descoberta de fármacos, evidência do mundo real e propriedade intelectual farmacêutica — e por que a primeira casa a entender isto vai redesenhar a economia da indústria.

VOLUME I · EDIÇÃO 2026 · CONFIDENCIAL

O que você vai *ler*.

Este eBook é um documento de decisão. Foi escrito para ser lido em uma reunião de comitê executivo, em uma viagem de avião, ou em um sábado de manhã antes de uma decisão de investimento de longo prazo.

00	Sumário Executivo	3
	<i>O argumento em uma página</i>	
I	A Indústria do Dado que Cura	5
	<i>Por que pharma virou — sem perceber — a maior operação de dado clínico sensível do planeta</i>	
II	O Cerco Regulatório	9
	<i>HIPAA, GDPR, ICH-GCP, FDA, EMA, Anvisa — e o fim da era da anonimização performática</i>	
III	FHE em Linguagem Executiva	13
	<i>O que é, sem matemática — e por que muda a economia da indústria</i>	
IV	Casos de Uso por Área	17
	<i>Ensaio clínico, RWE, descoberta, oncologia, raras, biológicos, manufatura, farmacovigilância</i>	
V	A Economia do Estudo Invisível	29
	<i>Custos reais, ROI, e onde aparecem os bilhões</i>	
VI	Vantagem Competitiva e Posicionamento	35
	<i>Por que isto é arquitetura regulatória, não TI</i>	
VII	Roadmap de 24 Meses	39
	<i>Da fase de aprendizado ao primeiro estudo público</i>	

VIII	Riscos, Mitigações e Armadilhas	45
	<i>O que pode dar errado e como evitar</i>	
IX	Manifesto	49
	<i>Uma carta para a próxima década da medicina baseada em dado</i>	
	Apêndices	53
	<i>Glossário, fornecedores, 30 perguntas para o CSO/CIO</i>	

O argumento em *uma* página.

Se você só vai ler uma coisa deste eBook, leia isto.

A indústria farmacêutica global enfrenta, simultaneamente, a maior oportunidade científica e o maior gargalo operacional da sua história. De um lado, a explosão de dado clínico, genômico, real-world e de imagem cria condições para uma medicina de precisão sem precedentes. Do outro, esse mesmo dado é tão sensível, tão regulado e tão proprietário que se torna estruturalmente inutilizável fora dos silos onde foi criado.

Cada grande farmacêutica do mundo opera hoje sobre uma contradição central: **tem mais dado do que jamais teve, e pode usar menos dele do que deveria.** Ensaios clínicos custam dois bilhões de dólares e levam uma década porque cruzar dados entre centros é juridicamente pesado. Real-world evidence é a obsessão regulatória da década, mas depende de dado de pagador, hospital e farmácia que ninguém pode juntar nominalmente. Descoberta de fármacos colaborativa é o futuro óbvio, mas exige duas farmas dividirem bibliotecas que nenhuma das duas confia ao concorrente.

Ao mesmo tempo, três forças estão convergindo:

1

REGULAÇÃO APERTANDO

HIPAA, GDPR, LGPD, ICH-E6(R3), EHDS europeu — todos exigindo prova matemática de minimização e provenance, não promessa de governança.

2

RWE COMO MANDATO

FDA, EMA e Anvisa aceitando real-world evidence como suporte regulatório — mas exigindo qualidade e governança que hoje quase ninguém entrega.

3

FHE MADURO

4

JANELA ABERTA

Lattigo, OpenFHE, Concrete em produção. Casos de uso reais (MELLODDY, Owkin, Roche) já demonstrando viabilidade técnica e econômica.

Nenhuma top 10 cravou ainda capacidade interna estruturada de computação privada. Quem chegar primeiro define o padrão que os demais seguem.

A tese deste eBook é direta:

“A próxima década da farma será definida por quem aprender primeiro a colaborar sem confiar — sobre dado clínico, genômico e proprietário, sem nunca decifrá-lo.”

FHE — *Fully Homomorphic Encryption* — é a tecnologia que torna isto matematicamente possível. Não é uma promessa de governança. É um teorema. O servidor que computa sobre dado de paciente cifrado **não tem como ver** o dado, mesmo se quiser, mesmo se for invadido, mesmo sob ordem judicial.

O custo computacional é alto e será discutido com honestidade. Mas para uma indústria onde um único ensaio fase III custa dois bilhões, onde uma única molécula salva ou destrói trimestres inteiros, e onde a vantagem competitiva mora em propriedade intelectual e dado proprietário — o cálculo já fechou. A pergunta para o conselho não é mais "se" investir em computação privada. É "qual será nosso primeiro caso de uso âncora, e quando começamos".

A DECISÃO

Não é "se" a indústria farmacêutica vai adotar computação privada. É "quem" vai liderar a definição do padrão setorial e capturar a vantagem regulatória, científica e competitiva da próxima década.

A Indústria do *Dado que Cura*.

Como uma indústria centenária de moléculas e ensaios se transformou — sem decreto e sem manifesto — em uma das maiores operações de dado clínico, genômico e biométrico do planeta. E como esse mesmo dado virou, ao mesmo tempo, ativo central e maior passivo operacional.

Em 2005, quando uma das grandes casas farmacêuticas conduzia um ensaio clínico fase III, o trabalho era essencialmente um exercício de logística médica. Centenas de centros distribuídos pelo mundo, milhares de pacientes recrutados, papelada física, monitoramento por visitas presenciais, dados consolidados em planilhas, análise estatística no fim. Custoso, sim. Lento, sim. Mas tecnicamente compreensível, juridicamente claro, e operacionalmente bem entendido.

Em 2025, o mesmo ensaio é uma operação de dados em tempo real. Wearables enviam dados contínuos do paciente diretamente ao sistema do estudo. Imagens de ressonância são processadas automaticamente por modelos de IA. Genoma é sequenciado nos primeiros 30 dias. Biomarcadores são monitorados por telemedicina. Cada paciente gera, ao longo do ensaio, entre 50 e 500 vezes mais dado do que há vinte anos. E cada um desses pontos de dado é potencialmente identificável, eternamente sensível, e juridicamente carregado.

Essa transformação aconteceu sem que os modelos de governança, a arquitetura técnica e a relação entre farmacêutica, hospital, pagador e paciente acompanhassem. O resultado é uma indústria que tem mais dado do que jamais teve, opera sob regulação cada vez mais agressiva, e ainda assim depende de uma arquitetura de privacidade que foi desenhada para um mundo que não existe mais.

O que mudou na cadeia de valor

Pharma sempre foi uma indústria de propriedade intelectual sustentada por ensaios clínicos. O que mudou nos últimos dez anos não é a estrutura dessa cadeia — é que cada elo dela virou uma operação de dado em escala industrial. Os cinco novos ativos:

ATIVO	O QUE É	RISCO
Prontuário eletrônico	Histórico clínico de paciente em ensaio ou em RWE study	Categoria especial · cadeia de custódia frágil
Genômica e ômicas	Sequenciamento de DNA, RNA, proteoma, metaboloma, microbioma	Identificação eterna · revela parentes não consentidos
Imagem médica	RM, TC, PET, retinografia, anatomopatologia digital	Re-identificação por traços faciais ou padrões raros
Real-world data	Claims, dispensações, prontuários ambulatoriais, wearables	Cruzamento entre fontes vazadas reconstrói o paciente
Bibliotecas de molécula	Estruturas químicas, dados de screening, ADMET, alvos	Propriedade intelectual de centenas de milhões em valor

Nenhum desses cinco ativos existia, em escala, na operação farmacêutica em 2010. Em 2026 são os cinco pilares da operação científica de qualquer top 20.

O que ninguém disse ao paciente

O paciente que assina um TCLE de ensaio clínico hoje não compreende, em qualquer sentido prático, o que está entregando. Ele acredita estar autorizando uma intervenção médica controlada — e está. Mas também está autorizando que seu genoma seja armazenado por décadas em servidor de uma multinacional, que sua imagem médica seja usada para treinar modelos de IA, que seu wearable transmita dados contínuos para sistemas em três continentes diferentes. O TCLE diz isso de alguma forma. Mas dizer não é compreender, e a indústria opera, hoje, sobre essa diferença de compreensão.

Esta é a parte difícil. E é a parte que vai colapsar primeiro, porque é a parte sobre a qual o regulador europeu já começou a se mover.

O PROBLEMA SILENCIOSO

A indústria farmacêutica opera, hoje, dependendo de uma cadeia de confiança entre paciente, médico, sponsor, CRO, fornecedor de tecnologia, e nuvem — que tem dezenas de pontos onde o dado existe em claro. Cada um desses pontos é um ponto de falha. E a regulação está, finalmente, começando a contar os pontos.

O paralelo histórico — e por que pharma é diferente

A indústria de redes sociais já passou pelo seu Cambridge Analytica. A indústria financeira já passou pelo seu Equifax. A indústria de saúde ainda não passou pelo seu evento, mas a pressão acumulada é maior do que ambas anteriores combinadas — porque dado clínico e genômico são, juridicamente e moralmente, a categoria mais protegida que existe.

A diferença é que a indústria farmacêutica tem, ao contrário das outras duas, uma vantagem estrutural: **a relação com o paciente é, no fundo, sobre cura.** Pharma pode escolher ser confiável de forma demonstrável. Pode escolher ser a primeira a dizer "nós coordenamos pesquisa entre cinco hospitais sem nunca ver o paciente individual de nenhum". Esse movimento — feito a tempo — é vantagem competitiva e regulatória simultânea. Feito tarde, é capítulo de livro de crise.

“A pergunta para qualquer comitê executivo de farma não é se a arquitetura atual de dado é sustentável. É quanto tempo falta até deixar de ser.”

O Cerco *Regulatório*.

Quatro continentes, dezenas de regulações, uma direção comum: o fim da era em que anonimização e governança contratual eram defesas suficientes.

Existe um equívoco confortável compartilhado pela maior parte da liderança jurídica das grandes farmas: o de que a regulação atual de dado clínico, embora pesada, pode ser administrada com base nas defesas tradicionais — TCLE bem escrito, anonimização técnica, contratos com CROs, cláusulas de transferência internacional, DPO competente. Esta visão é correta para 2020. Está errada para 2026.

HIPAA — quando a anonimização deixa de ser suficiente

O HIPAA americano permitiu, por décadas, que dado clínico fosse compartilhado em forma "de-identified" — removidos os 18 identificadores diretos. Esta defesa funcionou em um mundo onde re-identificação exigia esforço substancial e bases externas eram raras. Esse mundo acabou. Vários estudos publicados nos últimos cinco anos demonstraram re-identificação de "dados anonimizados" com taxas acima de 80% usando apenas três a cinco atributos quase-identificadores cruzados com bases públicas.

O resultado prático: HHS já abriu múltiplas investigações contra centros médicos e fornecedores de tecnologia por uso de "dados anonimizados" que foram re-identificados. A defesa de "removemos os 18 identificadores" não é mais defesa — é evidência de que se tentou minimizar sem entender o problema.

GDPR e a interpretação europeia

O GDPR é mais exigente. Dado de saúde é categoria especial sob o artigo 9, exigindo base legal específica e robusta. As autoridades nacionais europeias — CNIL francesa, Garante italiana, AEPD espanhola, ICO britânica — já produziram dezenas de decisões sancionando projetos de pesquisa farmacêutica por base legal frágil ou anonimização insuficiente. Multas em milhões de euros, e mais importante: **ordens de cessação de tratamento** que paralisaram estudos em andamento.

Em 2024 entrou em vigor o EHDS — European Health Data Space — que permite uso secundário de dado clínico para pesquisa, mas **exige arquitetura de governança técnica** que hoje quase nenhuma farma tem implementada. EHDS é o instrumento que, em três anos, vai redefinir quem pode operar pesquisa clínica na Europa. Quem não tiver capacidade de privacy-preserving analytics estará excluído por falta de qualificação técnica, não por falta de dinheiro.

ICH-E6(R3) — a virada operacional

A revisão ICH-E6(R3), publicada em 2023, marca uma mudança fundamental nas Boas Práticas Clínicas globais: pela primeira vez, a documentação técnica e de privacidade de um ensaio precisa demonstrar minimização **verificável**, não declarada. Reguladores começaram a perguntar, em inspeções, "como vocês *provam* que o sponsor não acessou dados individuais que não deveria"? A resposta de "temos uma política" não basta mais. A resposta certa será, em três anos, "temos uma arquitetura criptográfica auditável".

FDA, EMA, Anvisa e a aceitação de RWE

FDA, EMA e Anvisa aceitam, hoje, real-world evidence como suporte para decisões regulatórias — incluindo expansão de indicações e estudos confirmatórios pós-aprovação. Isto destrava bilhões em valor para sponsors, mas com uma contrapartida: o RWE precisa ter qualidade científica e governança de dado suficientes para sustentar a decisão. As três autoridades publicaram, nos últimos dois anos, guidance documents detalhando expectativas — e as expectativas convergem para um único princípio:

“Não basta dizer que o dado foi tratado com cuidado. É preciso provar matematicamente que ele não pôde ter sido tratado de outra forma.”

É exatamente neste ponto que FHE deixa de ser curiosidade técnica e vira **vantagem regulatória estrutural**. Uma farmacêutica que conduz seu RWE study sobre dado cifrado pode demonstrar à FDA,

EMA ou Anvisa — e ao comitê de ética — que o sponsor nunca acessou dados individuais, que o investigador local nunca viu dados de outros centros, que a análise estatística aconteceu sem que ninguém pudesse ter intervindo nos dados antes do lock. Isto não é uma política. **É um teorema verificável por terceiro.**

Brasil, China, Índia — a fragmentação regulatória

A LGPD brasileira tem o artigo 11 que coloca dado de saúde como categoria especial — equiparável ao GDPR no rigor formal, embora ainda imatura em jurisprudência. A ANPD começou a sinalizar, em 2025, fiscalização específica sobre pesquisa clínica. A China tem PIPL, talvez a lei mais agressiva do mundo em transferência internacional de dado de saúde — qualquer dado coletado em paciente chinês precisa passar por avaliação de segurança nacional para sair do país. A Índia tem o Digital Personal Data Protection Act, novo e em fase de regulamentação, mas claramente seguindo o modelo europeu.

Para uma farmacêutica global isto significa que a operação atual depende de manter **cinco a oito arquiteturas regulatórias paralelas**, cada uma com sua governança específica, sua localização de dado, suas restrições de transferência. É operacionalmente caro e estrategicamente frágil — qualquer mudança em uma jurisdição cria onda de retrabalho nas demais.

A JANELA ESTRATÉGICA

Reguladores estão buscando casos de uso "exemplares" de privacy-preserving research para citar em diretrizes e decisões. A primeira top 10 a apresentar arquitetura FHE auditável para RWE ou ensaio clínico vira citação oficial nas três grandes autoridades — proteção regulatória + posicionamento competitivo em uma única jogada.

O custo de não agir, em números

RISCO	PROBABILIDADE 5 ANOS	IMPACTO TÍPICO
Multa GDPR/LGPD por uso secundário sem base legal	Alta	2–4% do faturamento global
Paralisação de ensaio em andamento por DPA europeia	Média	Atraso de 6–18 meses no programa
Rejeição de submissão regulatória por falha de governança de dado	Média-alta	Atraso de 12–24 meses na aprovação
Class action nos EUA por uso de dado sem consentimento robusto	Média	USD 500M–2B (precedentes)
Exclusão de consórcios europeus por incapacidade técnica	Alta na UE	Perda de acesso a EHDS e a centros de excelência
Breach de dado clínico de paciente em ensaio	Média	Crise reputacional 24–48 meses + custos litigiosos

FHE em Linguagem *Executiva*.

Sem matemática. Sem jargão. Apenas o que a alta gestão precisa entender para tomar uma decisão de US\$ 50 milhões.

Imagine um cofre transparente. Você consegue ver que há algo dentro, mas não consegue ver o que é. Agora imagine que você consegue, de fora do cofre, com luvas matemáticas, manipular o conteúdo: somar duas coisas que estão lá, multiplicar, comparar, computar regressões, treinar modelos. Você executa operações sobre o conteúdo do cofre sem nunca abri-lo. Quando termina, devolve o cofre fechado para o dono da chave, que abre e vê o resultado. Isto é Criptografia Totalmente Homomórfica, em uma frase.

O salto conceitual

Toda criptografia que sua empresa usa hoje — TLS no portal, AES nos backups, HTTPS nas APIs — protege dado em *dois* dos três estados possíveis:

- **Em trânsito** — entre dispositivos. Resolvido por TLS.
- **Em repouso** — armazenado. Resolvido por AES.
- **Em uso** — quando o servidor processa. *Aqui o dado precisa estar em claro.*

O terceiro estado é o calcanhar de aquiles de toda arquitetura de privacidade clínica da história. Quando o sistema do ensaio calcula a estatística parcial, ele *precisa* ver os dados dos pacientes. Quando o modelo de IA roda sobre o exame, ele *precisa* ver a imagem. É nesse instante que o dado é vulnerável a funcionário desonesto, a invasão, a backup mal-configurado, a log mal-rotacionado, a subpoena, a CRO descuidada, a integração frágil entre fornecedores.

FHE elimina o terceiro estado. O servidor processa o dado **sem nunca ter acesso ao plaintext**. Esta é uma mudança de fase, não uma melhoria incremental.

Como funciona, em uma analogia que aguenta escrutínio

O mecanismo matemático real envolve reticulados (lattices) e o problema RLWE — o mesmo problema sobre o qual a próxima geração de criptografia pós-quântica é construída. Mas a intuição executiva é a seguinte:

ANALOGIA

O hospital "tranca" os dados de seus pacientes em uma caixa matemática usando uma chave que só ele tem. Envia a caixa fechada para o servidor do estudo multicêntrico. O servidor — que *nunca* recebe a chave — executa todo o algoritmo de análise estatística (média, variância, regressão, sobrevida, modelo de IA) *sobre a caixa fechada*, produzindo uma nova caixa com o resultado, ainda fechada. Devolve para o sponsor. O sponsor, que tem outra chave (gerada via threshold cryptography), abre apenas o resultado agregado. Em nenhum momento da cadeia ninguém — nem o servidor, nem o sponsor, nem o hospital remoto — vê os dados individuais de nenhum paciente.

O que FHE oferece que nada mais oferece

TECNOLOGIA	O QUE PROMETE	O QUE FALHA
Anonimização HIPAA	"Removemos os 18 identificadores"	Re-identificação trivial via cruzamento; legalmente frágil
TEE (enclave de hardware)	"O chip isola"	Confia no fabricante; vários ataques laterais publicados
Federated Learning	"Dado fica no centro"	Gradientes vazam dado individual; já demonstrado em pesquisa clínica
Differential Privacy	"Adicionamos ruído"	Bom para estatística agregada, ruim para decisão individual de eficácia
Synthetic Data	"Dados gerados artificialmente"	Não captura cauda longa; causal inference frágil; não substitui dado real
FHE	"Servidor nunca vê em claro"	Custo computacional alto — mas decrescente

FHE é a única tecnologia desta lista cuja garantia é **matemática e auditável por terceiro**. Para FDA, EMA, ANPD ou um comitê de ética europeu, é a diferença entre "acreditar na governança" e "verificar matematicamente".

Os três sabores que importam

CKKS

APROXIMADO · NÚMEROS REAIS

O sabor para machine learning, análise estatística, processamento de imagem

BFV/BGV

EXATO · INTEIROS

O sabor para banco de dados clínico cifrado, contagens exatas, estratificação. Quando o resultado precisa ser idêntico ao do plaintext.

médica. Permite multiplicações sobre vetores grandes. Lattigo e OpenFHE implementam.

TFHE

BOOLEANO · ULTRAFINO

Lógica bit-a-bit, comparações, programas arbitrários. Mais lento por operação, mas o mais flexível. Ideal para decisões clínicas de elegibilidade.

Híbrido

NA PRÁTICA

Sistemas reais combinam dois ou três. Inferência radiológica em CKKS, contagens de evento em BFV, elegibilidade em TFHE.

O mito do custo: o que você precisa saber

O argumento padrão contra FHE é "é caro demais". Em 2018, isto era verdade. Em 2026, é uma meia-verdade que precisa ser desmontada com cuidado:

- **O custo caiu duas a três ordens de magnitude** em sete anos. A curva é constante.
- **Para análise estatística sobre coorte clínica** (médias, variâncias, regressão logística, Kaplan-Meier sobre milhares de pacientes), latência hoje é de minutos a poucas horas — comercialmente viável para qualquer estudo cuja análise interim acontece em ciclos semanais.
- **Aceleradores de hardware** (Intel HEXL, FPGAs, ASICs específicos) prometem outro 10–100× nos próximos 24 meses.
- **O modelo certo é seletivo**: usar FHE no núcleo sensível (cruzamento de centros, agregação de gradientes federados, scoring de elegibilidade) e manter a operação trivial em claro local. Isto reduz o custo total a uma fração do orçamento atual de TI clínica.

O custo de FHE não é uma barreira. É uma **variável de design**. Para uma indústria que rotineiramente investe US\$ 2 bilhões em um único ensaio fase III, o overhead computacional de FHE em casos onde ele faz diferença real é, literalmente, ruído na planilha.

Casos de Uso por *Área*.

O que muda concretamente em cada vertical da operação farmacêutica. Ensaio clínico, RWE, descoberta, oncologia, raras, biológicos, farmacovigilância, manufatura — cada um com sua oportunidade específica e cada um com seu ROI distinto.

Ensaio clínico descentralizado

Ensaio descentralizado (DCTs) são a maior transformação operacional da indústria nos últimos cinco anos. O paciente em casa, o wearable, a telemedicina, o app de PRO. Tudo isso gera dados ricos, contínuos, e juridicamente carregados em volume sem precedentes.

Casos de uso FHE:

1. MONITORAMENTO CONTÍNUO SOB CIFRA

O wearable do paciente cifra os dados localmente antes de enviar. O sistema do estudo computa alertas pré-definidos (eventos adversos, deterioração clínica, abandono iminente) sobre a cifra. O monitor do estudo recebe apenas os alertas relevantes, nunca o dado bruto. **O sponsor nunca vê dado contínuo de paciente individual** — apenas as métricas agregadas e os alertas que justificam intervenção. Isto resolve, de uma vez, o problema do "muita gente do sponsor pode ver tudo dos pacientes".

2. ANÁLISE INTERIM SOB CIFRA

Análises de futilidade e eficácia interim são momentos críticos do ensaio. Hoje exigem desbloqueio parcial da base, com toda a complexidade de governança. Com FHE, a análise interim acontece sobre o ciphertext, e apenas a estatística final é decifrada (via threshold key compartilhada entre DSMB e sponsor). Resultado: análises interim mais frequentes, com menos risco de unblinding involuntário.

3. PRO E DADO EMOCIONAL

Patient-reported outcomes capturam dado psicológico, comportamental e de qualidade de vida. Esses dados são especialmente sensíveis e a tendência é o paciente subreportar quando sabe que será visto.

Coletar PRO sob cifra garante ao paciente que ninguém verá sua resposta individual — o que aumenta veracidade e adesão. Vários estudos preliminares mostram que coleta privada eleva taxa de resposta em 20–40%.

Real-world evidence (RWE)

RWE é o santo graal regulatório da década. FDA, EMA e Anvisa aceitam RWE como suporte para decisões — desde que a qualidade do dado e a governança sejam suficientes. Esta é a área onde FHE tem o maior ROI imediato, porque destrava casos hoje juridicamente impossíveis.

1. CRUZAMENTO ENTRE SPONSOR, HOSPITAL E PAGADOR

Para provar que um medicamento funciona "no mundo real", é preciso cruzar dispensação (farmácia/pagador), uso (prontuário hospitalar), e desfecho (clínico). Cada um pertence a uma entidade diferente, e nenhuma das três pode entregar o dado nominal às outras. FHE permite o cruzamento sem qualquer das partes ver o dado individual das outras. Resultado: estudos de RWE que hoje não acontecem porque não há base legal — passam a acontecer com base legal sólida.

2. COMPARATIVE EFFECTIVENESS

Comparar dois medicamentos no mundo real exige ajuste por confundidores observados — idade, sexo, comorbidades, terapias prévias. Cada um desses ajustes precisa de dado individual. Sob FHE, o ajuste estatístico (propensity score, IPTW, doubly robust) acontece sobre dados cifrados, sem que ninguém precise ver o paciente.

3. ESTUDOS PÓS-COMERCIALIZAÇÃO EXIGIDOS POR REGULADOR

FDA e EMA frequentemente exigem, como condição de aprovação, estudos de segurança pós-comercialização. Esses estudos hoje são caros e lentos porque envolvem múltiplos centros e pagadores. FHE reduz drasticamente o tempo até a primeira análise, porque elimina a necessidade de DUAs (data use agreements) bilaterais negociados por meses.

Descoberta de fármacos

1. BIBLIOTECAS QUÍMICAS COMPARTILHADAS

O caso mais célebre de computação privada em pharma é MELLODDY — consórcio de dez farmas (Janssen, Bayer, Boehringer, Novartis, Servier, AstraZeneca, GSK, Merck KGaA, Amgen, Astellas) que treinou modelos de bioatividade em federated learning sobre suas bibliotecas combinadas, sem

nenhuma delas ver os dados das outras. MELLODDY usou federated learning sem FHE — o que ainda permite vazamento parcial via gradientes. **A próxima geração desse tipo de consórcio será FHE-secured**, e a primeira casa a se posicionar como líder técnico desse movimento captura a relação central com todas as outras.

2. SCREENING VIRTUAL EM NUVEM SEM EXPOR IP

Pharma quer rodar simulação molecular pesada (docking, MD, QSAR) em GPU de nuvem (AWS, Azure, GCP), mas a fórmula é o ativo central. Hoje: ou roda on-prem (caro, lento) ou confia no cloud provider. FHE permite outsourcing de computação **sem revelar a entrada nem a saída**. CKKS é especialmente bom para simulação numérica.

3. COMPARTILHAMENTO DE DADOS NEGATIVOS

Dados de moléculas que *não* funcionaram são quase tão valiosos quanto os que funcionaram, e a indústria desperdiça bilhões duplicando experimentos negativos porque ninguém compartilha. Consórcio FHE de "dados negativos" é o tipo de iniciativa que economiza dinheiro sem entregar IP.

Oncologia — o caso mais sensível e mais valioso

Oncologia é onde tudo converge: dado genômico do tumor, imagem (anatomopatologia digital, RM), comorbidades, medicação, desfecho de longo prazo. Doença grave, paciente identificável por características raras, valor científico altíssimo, sensibilidade jurídica máxima.

1. TUMOR BOARDS MULTICÊNTRICOS SOB CIFRA

Tumor board internacional sobre caso oncológico complexo: 4 oncologistas em 4 países discutem o caso. Hoje: troca de e-mails desidentificados, com cadeia de custódia frágil. Com FHE: o caso circula cifrado, cada oncologista anota observações sobre cifra, ninguém precisa ver o nome do paciente. Aplicável tanto a casos individuais quanto a coortes.

2. INFERÊNCIA DE IA SEM ENVIAR O EXAME

Modelos de IA para predição de resposta a imunoterapia, identificação de variantes drivable, e estratificação de risco já existem. Hoje exigem que o paciente ou hospital envie o exame em claro para o servidor que hospeda o modelo. Na arquitetura correta, a rede de extração de features (CNN pesado) roda *localmente no hospital*, produzindo um embedding denso que captura toda a informação diagnóstica. Apenas o embedding é cifrado e enviado. O vendor executa o classificador final sob FHE e devolve o score cifrado. **O vendor nunca vê o exame nem o embedding em claro** — é o padrão usado por Owkin, Lifebit e Mozaic em produção hoje.

3. ESTUDOS GENÔMICOS COLABORATIVOS EM CÂNCER RARO

Câncer raro tem pacientes em volume tão pequeno que nenhum hospital tem coorte suficiente isoladamente. Cruzar bases é juridicamente pesado em qualquer jurisdição. FHE permite o estudo cruzado sem mover dado, e — mais importante — sem precisar do consentimento secundário para "cruzamento" porque tecnicamente o cruzamento acontece sob cifra.

Doenças raras

Doenças raras compartilham com câncer raro o problema da coorte minúscula. A diferença é que a regulação para doenças raras é mais favorável (orphan drug status, fast track), e as farmas que dominam a categoria têm relação direta com as associações de pacientes. Há aqui uma janela específica:

FHE permite criar **registries internacionais de doença rara** onde pacientes contribuem dados cifrados via app, e farmas/pesquisadores acessam apenas estatísticas agregadas. A associação de pacientes mantém a chave. Isto resolve simultaneamente o problema científico (amostra) e o problema ético (controle do paciente). Várias associações já procuraram parcerias desse tipo — falta a contraparte técnica capaz de entregar.

Biológicos, biossimilares e terapia avançada

Terapia gênica, terapia celular CAR-T, biossimilares — segmentos onde o paciente é raro, o produto é caríssimo, e a evidência precisa ser acumulada sobre cada paciente individual ao longo de anos. RWE de longo prazo aqui não é luxo, é exigência regulatória.

FHE permite seguimento longitudinal de paciente CAR-T por 10 anos sem que ninguém precise armazenar prontuário acumulado em claro. O paciente mantém a chave, contribui dado periodicamente, recebe acompanhamento, e o sponsor obtém a evidência agregada exigida pela FDA — sem violar nada.

Farmacovigilância colaborativa

Detecção de evento adverso raro depende de correlacionar dados entre países, hospitais, pagadores e fabricantes. Nenhuma fonte sozinha tem amostra. Hoje a farmacovigilância opera sobre relatos voluntários e cruzamentos manuais — sistematicamente lenta para detectar sinais raros.

FHE permite uma rede global de farmacovigilância onde fontes de dado contribuem cifradas para um servidor neutro (talvez sob OMS ou ICH), e sinais de segurança são detectados estatisticamente sobre a

cifra. Isto reduz drasticamente o tempo até detecção de eventos raros — e salva vidas mensuráveis.

Manufatura e cadeia de suprimentos

Caso menos óbvio mas importante. Manufatura farmacêutica envolve dados de processo proprietários (parâmetros de fermentação, condições de cromatografia, perfis de impureza) que são propriedade intelectual de altíssimo valor — e que precisam ser compartilhados parcialmente com fornecedores (CDMOs), reguladores (FDA, EMA), e parceiros de qualidade.

FHE permite que CDMO e sponsor computem sobre dados de processo sem que nenhum dos dois revele o seu IP completo. E permite que dados de qualidade sejam reportados a regulador em forma agregada cifrada, com auditoria possível mediante chave compartilhada.

Evidência financeira e value-based contracting

Contratos baseados em desfecho (pagador paga apenas se o paciente responder) são a tendência da década. Exigem cruzamento contínuo entre dispensação (pagador), uso (hospital) e desfecho (clínico). FHE permite que esse cruzamento aconteça sem que sponsor ou pagador precisem ver o paciente individual — cumprindo o contrato sem violar privacidade.

A Economia do *Estudo Invisível*.

Os números reais. Quanto custa, quanto retorna, e onde o capital encontra o valor — em escala de indústria farmacêutica.

Toda decisão de investimento em alta gestão precisa passar por três peneiras: capex, opex recorrente, e valor presente líquido descontado a um custo de capital realista. FHE não é exceção. Mas ao contrário de tecnologias de escala de marketing ou e-commerce, em farma o cálculo precisa ser feito contra o pano de fundo correto: a indústria onde um único ensaio fase III custa US\$ 2 bilhões e onde uma única molécula define trimestres inteiros.

O custo de fazer (capex inicial)

COMPONENTE	INVESTIMENTO TÍPICO
Time fundador (1 cripto-engenheiro sênior, 2 ML eng, 1 PM clínico, 1 jurídico de privacidade clínica)	USD 1.5M – 2.5M / ano
Licenças e tooling (Lattigo open, Concrete commercial, OpenFHE)	USD 80k – 350k / ano
Infra: GPUs e CPUs com AVX-512, FPGA opcional, ambiente validado GxP	USD 500k – 1.5M inicial
Consultoria estratégica (Zama, Duality, Inpher, Owkin) para arquitetura	USD 300k – 800k
Estudo regulatório com escritório especializado em pesquisa clínica	USD 250k – 700k
Validação CSV (computer system validation) para uso GxP	USD 200k – 500k
Total ano 1	USD 3M – 6M

O custo de operar (opex anual recorrente)

ITEM	ESTIMATIVA ANUAL
Compute (FHE 100x–1000x mais caro que plaintext na operação central)	USD 1.5M – 4M
Time de manutenção (5–8 engenheiros + 1 advisor regulatório)	USD 2.5M – 4M
Auditoria anual de segurança e revalidação	USD 300k – 800k
Opex anual estabilizado	USD 4.3M – 8.8M

Para uma farmacêutica top 20, isto representa entre **0,02% e 0,08% do faturamento**. Para colocar em perspectiva: é menos do que a maioria das casas gasta em *uma única reunião regional de força de vendas*. Para uma top 5 global, é arredondamento do orçamento de R&D.

O retorno — onde o dinheiro reaparece

O ROI de FHE em pharma vem de seis vetores que precisam ser modelados separadamente, cada um com magnitude muito superior aos casos de outros setores:

1. Redução de tempo de ensaio clínico

O custo de oportunidade de cada mês de atraso em um ensaio fase III é tipicamente **USD 30M–100M em receita perdida** (especialmente em oncologia e doenças raras). FHE reduz tempo até primeira análise interim, reduz tempo de negociação de DUAs entre centros, e elimina retrabalho de governança. Estimativa conservadora: **1–3 meses por ensaio**. Para uma top 20 com 30 ensaios fase III ativos, isto é **USD 1B–10B em valor presente**.

2. Habilitação de RWE como ativo regulatório

RWE submetido para FDA/EMA é hoje rejeitado em 40–60% dos casos por insuficiência de governança ou qualidade. FHE eleva qualidade e provenance, aumentando taxa de aceitação. Cada submissão de RWE bem-sucedida vale entre USD 100M e USD 2B em expansão de indicação ou aprovação acelerada. Captura conservadora: **2–5 submissões adicionais por ano** em uma top 20 = **USD 200M–10B em valor incremental**.

3. Acesso a consórcios e EHDS

O European Health Data Space, em pleno funcionamento, vai exigir capacidade técnica de privacy-preserving analytics para acesso a dados secundários. Quem não tiver capacidade, será excluído. EHDS dá acesso a coortes de centenas de milhões de europeus. Valor estimado: **USD 500M–3B em pesquisa habilitada nos próximos 5 anos**.

4. Proteção de IP de bibliotecas químicas

O risco anual de vazamento de dados de bibliotecas (interno ou via fornecedor) é estimado em **USD 50M–500M de valor presente esperado**. FHE para HPC em nuvem reduz drasticamente este risco. Tratamento como hedge: **USD 30M–300M em valor segurador**.

5. Redução de custo de governança regulatória

Cada ensaio multicêntrico hoje gasta USD 500k–2M em governança de dado e DUAs. FHE elimina a maior parte deste custo por substituir governança contratual por governança técnica. Para uma top 20, economia anual estimada: USD 30M–100M.

6. Vantagem em parcerias estratégicas

Hospitais acadêmicos de tier 1 (MD Anderson, Mayo, Charité, Karolinska, Hospital das Clínicas) estão cada vez mais cautelosos em parcerias que exijam compartilhamento nominal. Sponsors com capacidade FHE viram parceiros viáveis em colaborações que concorrentes não podem entrar. Vale 5–10 parcerias estratégicas exclusivas em 36 meses, cada uma com valor entre USD 20M e USD 200M.

O caso de negócio resumido

~USD 5M

INVESTIMENTO ANO 1

~USD 7M

OPEX ANUAL ESTABILIZADO

USD 1B+

VALOR HABILITADO EM HORIZONTE 5 ANOS

100×+

ROI ESPERADO EM HORIZONTE 5 ANOS

“Em qualquer modelagem honesta para uma farmacêutica top 20, FHE é o investimento de transformação digital com maior assimetria de retorno disponível em 2026.”

Não porque seja certeza de retorno alto. Mas porque o downside é trivialmente pequeno (custo conhecido, perfeitamente orçável) e o upside é estruturalmente assimétrico — cada um dos seis vetores acima, isoladamente, justifica o investimento. Os seis somados o tornam um dos investimentos óbvios da década.

Vantagem Competitiva e *Posicionamento.*

Em pharma, FHE não é primeiro narrativa — é primeiro vantagem regulatória e científica. A narrativa vem depois, e é consequência.

Há uma diferença importante entre a tese de FHE para cosméticos e a tese de FHE para farma. Em cosméticos, o valor central é narrativa de marca — "nós nunca vemos seu rosto" é uma promessa que vende crème caro. Em farma, a narrativa é secundária. O valor central é **capacidade operacional e regulatória que destrava casos hoje impossíveis**. A primeira casa a dominar FHE em pharma não vai vender mais por causa de campanha. Vai aprovar mais drogas, mais rápido, em mais indicações, com menos atrito regulatório. Isto vale exponencialmente mais do que qualquer narrativa.

Os três tipos de vantagem que FHE destrava

Vantagem regulatória

Quem apresenta primeiro uma submissão de RWE com arquitetura FHE auditável vira referência regulatória. FDA, EMA e Anvisa precisam de casos exemplares para citar em diretrizes — e o primeiro exemplo molda o padrão setorial. Não é exagero: a primeira top 20 a fazer isto vai influenciar o conteúdo das próximas três rodadas de guidance documents das três autoridades.

Vantagem científica

Quem domina FHE pode rodar estudos colaborativos que concorrentes não conseguem rodar. Câncer raro em coorte de cinco hospitais em três continentes, sem mover dado, sem anos de aprovação ética, sem fricção institucional. Pesquisas que hoje levam 5 anos saem em 18 meses. Isto se traduz em mais publicações, mais citações, mais reputação científica — e mais talento atraído.

Vantagem competitiva direta

Acesso a parcerias com hospitais acadêmicos de elite. Acesso a consórcios europeus via EHDS. Acesso a bibliotecas químicas compartilhadas. Acesso a registries internacionais de doença rara. Cada uma dessas portas se abre apenas para quem tem capacidade técnica de operar sob computação privada.

Os três posicionamentos possíveis

Posicionamento 1 — O Padrão Regulatório

Foco em virar referência setorial. Investimento pesado em publicar arquitetura, contribuir para guidance documents, participar de iniciativas multi-stakeholder com FDA, EMA, EHDS. A casa vira citação obrigatória. Funciona melhor para top 5 global com músculo regulatório significativo.

Posicionamento 2 — O Líder Científico

Foco em colaborações de elite com hospitais acadêmicos top 10 mundiais. A casa vira a parceira preferencial para estudos multicêntricos sensíveis. Funciona melhor para casas com forte presença em academia (Roche, Novartis, Merck KGaA, GSK).

Posicionamento 3 — O Especialista em Raras

Foco no segmento de doenças raras e câncer raro, onde FHE destrava casos genuinamente impossíveis. Constrói relação direta com associações de pacientes e registries internacionais. Funciona melhor para casas com portfólio em raras (Takeda, Sanofi Genzyme, Pfizer Rare Disease, Alexion).

Os três não são mutuamente exclusivos. Uma estratégia robusta combina os três em níveis diferentes da organização: posicionamento 1 no nível corporativo, posicionamento 2 nas unidades de R&D, posicionamento 3 nas business units específicas.

O custo de não posicionar

Há um cenário que precisa ser explicitado em conselho: o que acontece se nenhuma das top 20 adotar FHE estruturalmente nos próximos 36 meses?

Resposta: **os tech players vão fazer.** Owkin, Lifebit, Mozaic, ConcertAI, e novos entrantes vão oferecer "FHE-as-a-service para pharma" e capturar a posição intermediária. As top 20 vão acabar comprando esses serviços a múltiplos elevados — entregando dado, dependência operacional e captura de valor para fornecedores que poderiam ter sido construídos internamente. É exatamente o que aconteceu com a infraestrutura de IA clínica nos últimos cinco anos: quem terceirizou cedo, paga caro hoje. Quem não terceirizar agora, paga ainda mais caro em três anos.

“A escolha não é entre adotar FHE ou não. É entre ter capacidade interna ou alugá-la a múltiplos crescentes do tech.”

Roadmap de 24 Meses.

Da decisão do conselho ao primeiro estudo clínico submetido com arquitetura FHE auditável. Quatro fases, marcos claros, métricas de saída em cada uma.

01

MESES 1-6 · APRENDER

Fundação e capacidade interna

Contratar o cripto-engenheiro sênior fundador. Esta contratação é o gargalo real — há talvez 200 pessoas no mundo qualificadas. Recomendação: aquisição parcial de uma startup (Zama, Owkin, Inpher, Tune Insight) é frequentemente o atalho mais rápido. Em paralelo: contratar consultoria estratégica para arquitetura inicial. Reproduzir benchmarks públicos. Identificar três casos de uso candidatos com ROI claro e elegê-los para piloto.

Métrica de saída: arquitetura técnica documentada, três casos selecionados (idealmente um RWE, um ensaio clínico e um descoberta), parecer jurídico interno validando viabilidade em GDPR/HIPAA/LGPD.

02

MESES 7-14 · CONSTRUIR

Piloto interno em ambiente controlado

Construir um único caso de uso, ponta a ponta, em ambiente controlado.

Recomendação: análise estatística cifrada sobre coorte sintética que mimetiza um RWE study. Isto é o caso tecnicamente mais maduro e o de maior valor demonstrativo.

Validar latência, custo, precisão, fluxo de chaves, cadeia de auditoria. Em paralelo: começar a estruturar o material para diálogo regulatório.

Métrica de saída: demo funcional sobre coorte sintética, métricas validadas por terceiro independente, documentação técnica pronta para submissão a IRB e a regulador.

03

MESES 15-20 · ESTUDO REAL FECHADO

Primeiro estudo real, sob escrutínio ético controlado

Lançar o primeiro estudo clínico ou de RWE real usando a arquitetura. Sugestão: um estudo de pequeno porte em segmento bem dominado pela casa. Idealmente: doença rara ou câncer raro, onde o valor é mais óbvio. Pacientes consentem com a arquitetura nova explicitamente. IRB recebe documentação técnica completa. Resultado é validado contra estudo paralelo em arquitetura tradicional.

Em paralelo: começar diálogo formal com FDA, EMA e Anvisa sobre uso da arquitetura em submissões futuras. Engajar pre-submission meetings.

Métrica de saída: primeiro estudo real concluído, parecer favorável de IRB, primeiro feedback regulatório positivo de pelo menos uma das três autoridades.

04

MESES 21-24 · PADRÃO INTERNO

Adoção como capacidade institucional

Tornar a arquitetura disponível para múltiplos programas em curso. Treinar equipes de R&D em como propor FHE em desenhos novos. Publicar whitepaper técnico. Apresentar em DIA, ASCO, ESMO, conferências regulatórias. Submeter primeiro estudo formal usando a arquitetura como parte do pacote regulatório.

Esta é a fase em que o investimento dos 20 meses anteriores começa a gerar retorno em escala. Feita corretamente, gera reconhecimento setorial sustentado e posição

preferencial em colaborações futuras.

Métrica de saída: 3+ programas internos usando a capacidade, primeira submissão regulatória formal incorporando arquitetura FHE, reconhecimento em pelo menos uma diretriz pública de FDA/EMA.

Marcos que o conselho deve cobrar

MARCO	QUANDO	COBRANÇA
Cripto-engenheiro fundador contratado ou aquisição definida	Mês 4	Sem isto, não há projeto
Caso de uso selecionado e validado por jurídico clínico	Mês 6	Sem alinhamento jurídico, atrito eterno
Demo técnica funcional sobre coorte sintética	Mês 14	Prova de viabilidade real
Primeiro estudo real iniciado com IRB aprovado	Mês 18	Validação ética e técnica simultânea
Primeiro feedback regulatório positivo	Mês 22	Sinal de que o investimento se converte em vantagem regulatória

Riscos, Mitigações e Armadilhas.

O que pode dar errado, em ordem decrescente de probabilidade e gravidade.

Risco 1 · Não conseguir contratar talento fundador

Probabilidade: alta. **Impacto:** bloqueante.

Há talvez 200 pessoas no mundo qualificadas a liderar uma operação de FHE em produção. Quase nenhuma trabalha hoje em farma — vêm de Zama, Duality, Inpher, Tune Insight, Owkin, IBM Research, ou da academia. Convencer uma a entrar em farma é difícil porque o ciclo de validação em GxP é hostil ao perfil.

Mitigação: tratar como aquisição estratégica, não contratação. Acquire de uma startup é frequentemente o caminho mais rápido (ver Owkin, comprado pela Sanofi em 2025; Lifebit; Mozaic). Custo maior, time já formado, time-to-capability significativamente menor.

Risco 2 · Validação CSV e ambiente GxP

Probabilidade: média-alta. **Impacto:** manageable mas demorado.

Pharma opera sob ambientes validados (GxP, CSV, 21 CFR Part 11). Bibliotecas FHE não foram desenhadas para esse padrão. Validar o stack para uso GxP é um projeto não-trivial.

Mitigação: começar pelo uso não-GxP (descoberta, pré-clínico, RWE retrospectivo). Validar stack em paralelo com casos não-críticos. Migrar para GxP apenas quando o stack estiver maduro e o time confortável.

Risco 3 · Custo computacional não cair na velocidade prevista

Probabilidade: média. **Impacto:** manageable.

A curva de redução de custo de FHE depende de avanços algorítmicos e de hardware. Se o ritmo desacelerar, casos com volume muito grande de pacientes podem ser inviáveis temporariamente.

Mitigação: começar por casos de volume baixo e valor alto (raras, oncologia, biológicos). O caso desses segmentos se sustenta sozinho e não depende de mais reduções de custo.

Risco 4 · Regulador não entender ou rejeitar a arquitetura

Probabilidade: baixa-média. **Impacto:** alto.

Existe chance de FDA, EMA ou Anvisa interpretarem a arquitetura como insuficientemente auditável, ou pedirem garantias adicionais que tornam o uso impraticável.

Mitigação: engajar os reguladores **antes** do uso, em pre-submission meetings. Apresentar a arquitetura. Buscar parecer prévio. Co-construir o protocolo de auditoria. Reguladores que opinam favoravelmente viram aliados, não adversários.

Risco 5 · Concorrente anuncia primeiro

Probabilidade: média. **Impacto:** alto.

Roche, Novartis, Pfizer, Sanofi, Janssen — qualquer um pode estar com projeto similar em curso. Improvável que esteja no mesmo estágio, mas possível.

Mitigação: velocidade. Cada mês de atraso é um mês a mais de exposição ao risco. Considerar parcerias com vendor de FHE como aceleração em vez de construir tudo do zero.

Risco 6 · Vulnerabilidade descoberta no esquema FHE

Probabilidade: muito baixa. **Impacto:** médio-alto.

Esquemas FHE modernos são baseados em problemas de reticulado bem estudados — os mesmos problemas sobre os quais NIST padronizou a próxima geração de criptografia pós-quântica. A confiança matemática é alta. Mas avanços teóricos imprevistos sempre são possíveis.

Mitigação: usar parâmetros conservadores. Acompanhar a literatura. Ter plano de migração entre esquemas. Não usar FHE como única camada de defesa — combinar com TLS, AES, segregação de chaves, auditoria.

Armadilha 1 · Tratar como projeto de TI

O erro mais comum em adoção de tecnologia transformadora é colocá-la sob CIO/CTO em vez de sob CSO/Chief Medical Officer/Chief R&D Officer. Resultado: entrega técnica perfeita e impacto científico nulo. **FHE em farma deve reportar ao R&D ou ao CMO, com sponsor do CEO.**

Armadilha 2 · Começar pelo caso errado

A tentação é começar pelo caso de maior visibilidade — frequentemente um ensaio fase III em curso. É um erro. Casos críticos não toleram experimentação. Começar por descoberta, RWE retrospectivo, ou estudos investigador-iniciados, onde o risco é baixo e o aprendizado é rápido.

Armadilha 3 · Esquecer a governança de chave

FHE protege durante a computação. Mas o gerenciamento de chaves é onde a maioria das implementações falha. Para pharma, a estrutura certa envolve threshold cryptography compartilhada entre sponsor, IRB e parceiro independente — para que nenhuma parte sozinha possa decifrar. **O design da governança de chave é metade do projeto.**

Armadilha 4 · Subestimar o jurídico clínico

Jurídico clínico de farma é uma especialidade própria, distinta de jurídico de privacidade comercial. Engajar errado ou tarde resulta em retrabalho massivo. O jurídico precisa estar no projeto desde o mês 1.

Uma carta para a próxima década da *medicina baseada em dado*.

Para os CEOs, conselheiros, Chief Scientific Officers e Chief Medical Officers das casas que ainda podem escolher liderar.

A indústria que vocês lideram foi construída sobre uma promessa antiga e nobre: a de que a ciência aplicada à doença pode reduzir sofrimento humano em escala. Que descobrir uma molécula, validá-la em ensaios rigorosos, e levá-la ao paciente é um ato de cuidado coletivo que merece o capital, o talento e a confiança que a sociedade investe na indústria. Que o paciente que entra em um ensaio clínico não é matéria-prima, é parceiro — e que a relação entre sponsor e paciente, mediada por médico e investigador, é uma relação de confiança no sentido mais profundo da palavra.

Essa promessa atravessou um século. Sobreviveu a tragédias éticas (Thalidomida, Tuskegee, Estônia), sobreviveu a transformações técnicas (das pequenas moléculas aos biológicos, dos biológicos às terapias gênicas), sobreviveu à comoditização parcial pela genéricos. Sobreviveu porque era — e em grande parte ainda é — verdadeira. Os pacientes que entram em ensaios clínicos hoje têm uma relação de respeito e expectativa real com a indústria, mediada por médicos que confiam no sistema.

Mas nos últimos dez anos, sem que ninguém tenha decretado, a relação entre indústria e paciente mudou de natureza. O paciente deixou de ser quem assina um TCLE específico para um experimento específico, e passou a ser uma fonte contínua de dado: prontuário, genoma, imagem, wearable, comportamento, geolocalização, microbioma. Cada um desses dados nasceu com uma justificativa local — uma única decisão de inclusão de feature, um único protocolo, uma única integração. Mas o resultado agregado é algo que nenhum executivo individual conscientemente desenharia: uma operação de coleta de dado clínico íntimo em escala industrial, mediada por uma cadeia de fornecedores e provedores onde o dado existe em claro em dezenas de pontos, e onde a única defesa é uma frágil cadeia de confiança contratual.

É possível voltar atrás. Mais que isso: é estrategicamente preferível voltar atrás. Não porque a regulação exija — embora exija. Não porque um eventual breach seja inevitável — embora seja, eventualmente,

em algum lugar. Mas porque a relação original, baseada em respeito real ao paciente, era mais valiosa, mais sustentável, e mais alinhada com a missão central da indústria.

FHE — Criptografia Totalmente Homomórfica — é a primeira tecnologia em décadas que permite voltar atrás **sem perder as capacidades**. É possível continuar fazendo RWE study, continuar treinando modelos de IA sobre imagem médica, continuar conduzindo ensaios descentralizados, continuar fazendo descoberta colaborativa, continuar construindo registries internacionais. **É possível fazer tudo isso sem nunca ver o paciente individual.**

Esta frase parece, em uma primeira leitura, paradoxal. Em uma segunda leitura, parece técnica demais. Em uma terceira, parece o argumento mais óbvio que a indústria já teve à sua disposição. Como é possível pesquisar sem ver? A matemática responde — e a resposta é elegante, antiga, e finalmente viável em produção.

O que está em jogo não é uma feature técnica. É a possibilidade de uma indústria voltar a ser, sem ambiguidade, o que ela sempre disse ser: uma indústria de cura. Uma indústria que respeita o paciente como parceiro pleno, com privacidade matematicamente verificável e não com promessa de gestão. Uma indústria capaz de colaborar consigo mesma sem precisar entregar IP, capaz de compartilhar conhecimento sem entregar competitividade, capaz de cumprir o contrato regulatório com transparência matemática.

Esta possibilidade está aberta, hoje, para um número pequeno de casas globais. As primeiras a entender o que está em suas mãos. As primeiras a fazer a contratação certa, a chamar o jurídico certo, a apresentar o caso ao conselho certo. As primeiras a publicar a primeira submissão regulatória usando a arquitetura, as primeiras a engajar FDA e EMA em conversas formais, as primeiras a sustentar a posição em entrevista, em conferência, em artigo, por dois anos seguidos sem ceder à tentação de diluir a mensagem.

Em três anos, esta posição vai estar tomada. Algum player vai liderar — interno ou tech entrante. Pharma sempre teve a capacidade técnica e o capital para liderar suas próprias transformações; o que frequentemente faltou foi a coragem de mover antes que o problema virasse crise. Esta é uma janela diferente. É a primeira janela em que a indústria pode escolher liderar antes de ser pressionada — porque o problema regulatório ainda está se formando, mas a solução técnica já está pronta.

“A pergunta não é se a indústria vai mudar. É se vamos mudar liderando, ou liderados.”

Há uma janela. É curta. É real. É historicamente rara. Indústrias inteiras passam décadas esperando por janelas como esta — e a maioria das casas instaladas as perdem por excesso de prudência operacional. Pharma já passou por outras: a transição para biológicos (e algumas casas perderam para entrantes especializados), a transição para terapia gênica (e algumas perderam para startups que viraram unicórnios). Esta é a próxima. É possivelmente a última desta década com capacidade de redefinir a arquitetura central de como a indústria pesquisa, colabora e regula a si mesma.

Quem ler este eBook tem em mãos um mapa. O mapa não é completo, não é sem riscos, não é sem custos. Mas é claro. E está, neste momento, na frente das pessoas certas para tomar a decisão certa.

O resto é coragem.

— *Fim do Volume I*

Glossário *Executivo*.

Os termos que você vai ouvir do CSO/CIO. Em português direto.

FHE — FULLY HOMOMORPHIC ENCRYPTION

Criptografia que permite executar cálculos sobre dados cifrados sem decifrá-los. O resultado, quando decifrado, é igual ao que seria obtido sobre os dados originais.

RLWE — RING LEARNING WITH ERRORS

O problema matemático sobre o qual a maioria dos esquemas FHE modernos se baseia. É o mesmo problema da criptografia pós-quântica padronizada pelo NIST (ML-KEM, ML-DSA). Resistente a computadores clássicos e quânticos.

CKKS, BFV, BGV, TFHE

Os quatro principais esquemas FHE em uso prático. CKKS para ML e estatística; BFV/BGV para inteiros exatos; TFHE para lógica booleana flexível.

RWE — REAL-WORLD EVIDENCE

Evidência clínica derivada de dados de uso real (claims, prontuários, registries) em vez de ensaios controlados. FDA, EMA e Anvisa aceitam RWE como suporte regulatório quando a qualidade é suficiente.

EHDS — EUROPEAN HEALTH DATA SPACE

Iniciativa europeia que cria infraestrutura comum para uso secundário de dado clínico em pesquisa. Vigente em fases até 2027. Vai exigir capacidade técnica de privacy-preserving analytics como pré-requisito.

ICH-E6(R3)

Revisão das Boas Práticas Clínicas internacionais publicada em 2023. Marca a virada para exigência de governança de dado verificável, não apenas declarada.

CSV — COMPUTER SYSTEM VALIDATION

Processo de validação exigido pela FDA (21 CFR Part 11) e equivalentes para sistemas computacionais usados em operação GxP. FHE em ambiente clínico precisa passar por CSV.

GXP

Termo guarda-chuva para Good Manufacturing/Clinical/Laboratory Practice — padrões regulatórios que governam toda a operação farmacêutica. Sistemas usados em GxP têm exigências adicionais de validação, auditoria e rastreabilidade.

DSMB — DATA SAFETY MONITORING BOARD

Comitê independente que monitora segurança e eficácia em ensaios clínicos. Em ensaios sob FHE, o DSMB tem papel central no gerenciamento de chaves para análises interim.

THRESHOLD CRYPTOGRAPHY

Técnica que distribui uma chave criptográfica entre múltiplas partes, exigindo um quórum para usá-la. Essencial para arquitetura FHE em farma — nenhuma parte sozinha pode decifrar.

PSI — PRIVATE SET INTERSECTION

Protocolo derivado de FHE/MPC que permite duas partes descobrirem a interseção de seus conjuntos sem revelar o restante. Útil para identificar pacientes em comum entre centros sem expor bases.

FEDERATED LEARNING

Treinamento distribuído onde dado fica local. Quando combinado com FHE para agregação de gradientes (FL+FHE), elimina o vazamento que FL puro tem.

LATTIGO, OPENFHE, CONCRETE

Principais bibliotecas FHE em uso prático. Lattigo (Go, Tune Insight); OpenFHE (C++, Duality); Concrete (Rust+Python, Zama).

Fornecedores e *Parceiros*.

Onde está a capacidade comercial, onde está o talento, e onde já há casos de uso ativos em pharma.

Fornecedores e startups especializadas

VENDOR	SEDE	FOCO
Owkin	Paris / NY	FL+FHE para pesquisa clínica; adquirida parcialmente pela Sanofi
Zama	Paris	TFHE, Concrete framework, foco em developer experience
Duality Technologies	EUA / Israel	OpenFHE, foco em saúde e finanças, consultoria pesada
Inpher	Suíça / EUA	FHE + MPC híbrido, foco em finanças e saúde
Tune Insight	Suíça (EPFL)	Lattigo, foco em pesquisa médica federada
Lifebit	Reino Unido	Plataforma de federated genomics para farma
Mozaic / TripleBlind	EUA	Privacy-preserving analytics para pharma e payor
ConcertAI	EUA	RWE com governança avançada para oncologia

Iniciativas e consórcios relevantes

- **MELLODDY** — consórcio europeu de 10 farmas para descoberta colaborativa via federated learning (concluído; sucessor em FHE em discussão)
- **Trustworthy Federated Data Analytics (TFDA)** — Helmholtz, Alemanha — pesquisa clínica federada com privacidade
- **European Health Data Space (EHDS)** — infraestrutura europeia para uso secundário de dado clínico
- **NIH N3C** — National COVID Cohort Collaborative (modelo de governança aplicável)
- **Global Alliance for Genomics and Health (GA4GH)** — padrões para dado genômico, incluindo computação privada

Centros acadêmicos onde mora o talento

- **EPFL (Lausanne)** — Christian Cachin, Jean-Pierre Hubaux, origem do Lattigo
- **IBM Research** — origem histórica do FHE (Craig Gentry, 2009)
- **Microsoft Research** — biblioteca SEAL, Kim Laine
- **NJIT / Duality** — Yuriy Polyakov, Kurt Rohloff
- **Université Paris-Saclay / ENS** — Léo Ducas e o ecossistema francês
- **KU Leuven (COSIC)** — Frederik Vercauteren
- **Stanford / MIT / CMU** — vários pesquisadores ativos em ML+FHE clínico

30 Perguntas para o *CSO/CIO*.

A lista que você deveria levar para a próxima reunião com seu time científico e de tecnologia.

Estratégia e capacidade

1. Temos no time alguém com background em criptografia avançada? Se não, qual o plano?
2. Qual nossa exposição atual a tratamento de dado clínico, em volume e em jurisdição?
3. Quantos ensaios em curso processam dados em ambientes onde sponsor pode acessar dado individual de paciente?
4. Temos um inventário atualizado de quais dados saem do centro investigador e onde são processados?
5. Qual nosso parecer jurídico atual sobre sustentabilidade dessa arquitetura nos próximos 36 meses?

Casos de uso prioritários

6. Qual nosso programa de RWE de maior valor potencial — e qual o gargalo regulatório dele?
7. Quais ensaios em curso poderiam ter desenho descentralizado mais ambicioso se a privacidade fosse resolvida?
8. Em quais áreas terapêuticas a coorte é tão pequena que cruzamento internacional seria transformador?
9. Em que ponto da descoberta nossas bibliotecas químicas saem de ambiente totalmente controlado?
10. Temos bibliotecas que valeria compartilhar com concorrentes em consórcio se a privacidade fosse matemática?

Arquitetura técnica

11. Qual esquema FHE faz mais sentido para nosso primeiro caso? CKKS, BFV, TFHE?
12. Qual a profundidade computacional do nosso pipeline analítico mais valioso?

13. Conseguimos rodar uma análise estatística básica (médias, variâncias, regressão) em FHE com latência aceitável hoje?
14. Qual seria o overhead computacional estimado para nosso caso?
15. Como gerenciamos chaves entre sponsor, IRB, DSMB e parceiros?
16. Quem custodia a chave em caso de DSMB internacional?
17. Temos arquitetura compatível com threshold cryptography?

Custo e infraestrutura

18. Custo computacional estimado por análise, em FHE versus plaintext?
19. Que aceleradores avaliamos? FPGA? GPU específico? AVX-512?
20. Vamos construir interno ou usar vendor (Owkin, Zama, Duality)?
21. Qual o capex e opex previstos nos próximos 24 meses?
22. Como integramos com nossa stack atual de eCRF, EDC e CTMS?

Regulação e validação

23. Os parâmetros de segurança atendem 128 bits e são pós-quânticos?
24. Quem fará a auditoria de segurança independente?
25. Como demonstramos conformidade com HIPAA, GDPR, LGPD, ICH-E6(R3)?
26. Conseguimos publicar a arquitetura para revisão pública e regulatória?
27. Já temos diálogo aberto com FDA, EMA ou Anvisa sobre o uso?
28. Como passamos por CSV/21 CFR Part 11 para uso GxP?

Riscos

29. Pior cenário se um competidor anunciar antes de nós?
30. Pior cenário se o regulador pedir garantias técnicas que ainda não conseguimos entregar?



O Ensaio Invisível

eBook estratégico para a alta gestão da indústria farmacêutica global.

Volume I · Edição 2026 · Distribuição confidencial.

Composto em Iowan Old Style e SF Pro.

Construído como documento HTML auto-contido.

Imprima em papel de gramatura alta para fidelidade ao layout original.

— fim —