### **Evaluación Crítica de Idea: Historial Clínico Descentralizado para Seguros**

**1. VEREDICTO DE VIABILIDAD (36H):** ELEGIDO

**2. Análisis del Problema y Relevancia Social**

* **Problema Real (Bolivia/LATAM):** El problema es fundamental y muy relevante. La portabilidad y propiedad de los datos médicos por parte del paciente es prácticamente inexistente. Los historiales están fragmentados y controlados por las clínicas, creando un proceso burocrático y lento para que los pacientes accedan a su propia información y la compartan con aseguradoras u otros proveedores de salud.
* **Beneficiarios Claros:**
  1. **Pacientes:** Ganarían soberanía sobre su historial médico, pudiendo compartirlo de forma selectiva y segura.
  2. **Aseguradoras Privadas:** Podrían agilizar drásticamente sus procesos de evaluación de riesgos y suscripción de pólizas al recibir acceso directo y consentido a la información verificada.
* **Impacto Potencial:** Transformador. Un sistema así podría rediseñar la infraestructura de datos de salud, reducir costos administrativos y empoderar a los pacientes. Sin embargo, su enorme potencial está directamente relacionado con su enorme complejidad técnica.

**3. Propuesta de MVP y Arquitectura para 36 Horas**

* **MVP Mínimo y Realista:** Incluso el MVP más básico de esta idea es engañosamente complejo y excede la ventana de 36 horas. Un demo funcional requeriría, como mínimo:
  1. **Flujo de Cifrado:** El usuario debe poder cifrar un archivo (ej. un PDF con un resultado de laboratorio) en el lado del cliente (en el navegador) antes de subirlo.
  2. **Almacenamiento:** El archivo cifrado se sube a IPFS.
  3. **Registro On-chain:** Un Smart Contract registra el hash de IPFS y, crucialmente, la lógica de permisos.
  4. **Control de Acceso Delegado:** El paciente (dueño de los datos) necesita una interfaz para conceder permiso de lectura a otra dirección (la aseguradora).
  5. **Flujo de Descifrado:** La aseguradora debe poder usar el permiso concedido on-chain para descifrar y ver el archivo original.
* **Arquitectura Técnica Sugerida:** La pila parece estándar (React, IPFS, Solidity), pero el diablo está en los detalles del control de acceso.
  + **El Punto Crítico:** El mecanismo de cifrado y descifrado delegado (pasos 4 y 5) es el núcleo del proyecto. Esto no es una simple transacción. Requiere implementar esquemas de criptografía de clave pública complejos, como ECIES (Elliptic Curve Integrated Encryption Scheme) o utilizar plataformas de terceros como **Lit Protocol**. Integrar y depurar estas soluciones para que funcionen de manera fluida para dos tipos de usuarios (paciente y aseguradora) es una tarea monumental.
* **Uso de Tecnología Descentralizada:** La justificación es impecable. La soberanía de datos del paciente es un caso de uso insignia de Web3. El problema es que un caso de uso conceptualmente perfecto no siempre se traduce en un proyecto viable para un buildathon.

**4. Cumplimiento de Reglas y Entregables**

* **Desarrollo desde Cero:** La idea se presta a ser construida desde cero.
* **Plan de Entregables (Estimación de Tiempo):**
  + Smart Contracts (con lógica de permisos y control de acceso): [Estimación] 10-14 horas
  + Lógica Core (Cifrado/Descifrado en cliente y delegación de claves): [Estimación] 20+ horas. **Este es el bloque que hace que el proyecto no sea viable.**
  + Desarrollo Frontend (UI para paciente Y aseguradora): [Estimación] 15-18 horas
  + **Total Estimado:** [Estimación] 45-52 horas. Esta estimación conservadora ya supera con creces las 36 horas disponibles, y asume que el equipo no encontrará ningún problema mayor en la compleja implementación criptográfica.
* **Riesgo Principal:** **Falla catastrófica en el flujo de descifrado.** El equipo puede pasar todo el fin de semana desarrollando y, al momento de la demo, el representante de la "aseguradora" no podrá ver el archivo. Sin ese paso final, la demo no tiene valor. [Inferencia] El riesgo de que esto ocurra es extremadamente alto, cercano al 100%, para un equipo promedio en un buildathon.

**5. Conclusión y Recomendaciones Estratégicas**

* **Valoración Final:** Esta es una idea excelente para una startup o un proyecto de investigación a largo plazo, pero es una candidata muy pobre para este buildathon. La complejidad técnica fundamental del control de acceso a datos cifrados está mucho más allá de lo que se puede construir, probar y demostrar de manera fiable en un solo fin de semana.
* **Sugerencia Crítica para el Equipo:** **PIVOTEEN INMEDIATAMENTE A UNA IDEA QUE NO REQUIERA CIFRADO DE DATOS CON ACCESO DELEGADO.** No intenten simplificar esta idea; su núcleo es la parte compleja. En su lugar, consideren un concepto relacionado pero más simple del espacio de identidad digital (SSI):
  + **Alternativa Viable:** Creen un sistema de **"Credenciales Verificables"** de salud. Un "Médico" (una dirección de wallet con un rol) emite una credencial on-chain (podría ser un Soulbound Token/SBT) a un "Paciente". La credencial no contiene datos sensibles, solo certifica un hecho (ej: "Certificado de Vacunación", "Miembro de Seguro X", "Tipo de Sangre O+"). El paciente simplemente muestra la posesión de esta credencial. Esto elimina por completo la gestión de archivos, el cifrado y el acceso delegado, pero aun así demuestra un poderoso caso de uso de identidad en Web3.