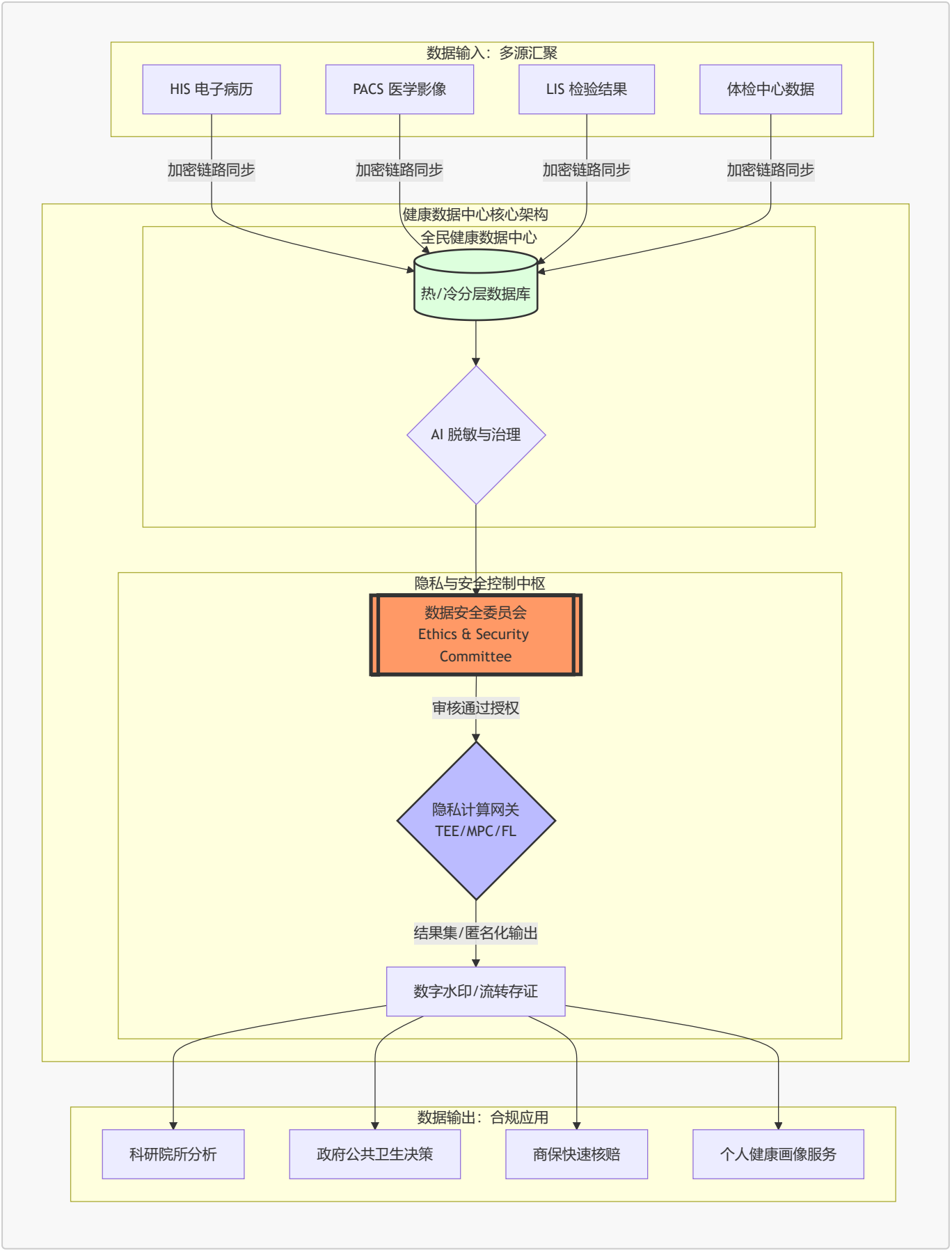
全民健康数据中心：安全与价值框架

1. 全局业务框架图（形象演示）

本框架展示了数据从“多源输入”到“中心治理”，再到经过“安全委员会审批”后通过“隐私计算控制”输出到应用端的全闭环逻辑。



2. 核心架构逻辑说明

2.1 高标准数据输入 (Input)

- **全量采集**：通过标准的 HL7/FHIR 协议，将全市范围内医院的门诊、住院、影像、检验数据实时或准实时同步至中心。
- **初级清洗**：在进入核心库前，AI 自动进行格式化校对和初步的身份唯一化关联。

2.2 强化版隐私控制 (Control) —— 核心关注点

本方案设计的隐私控制不仅是技术层面的，更是流程与组织层面的：

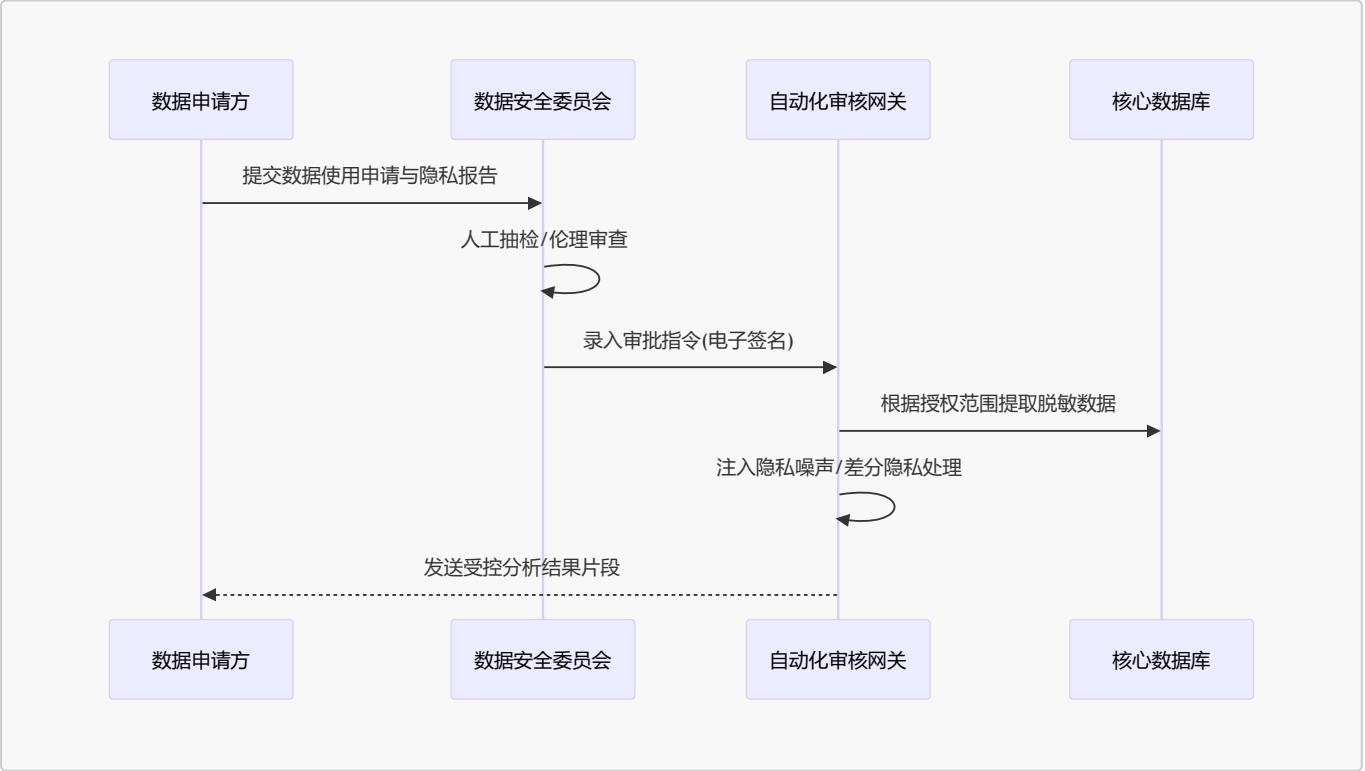
1. **数据安全委员会 (The Committee)**：
    - **组成**：由法律专家、伦理专家、技术专家和卫健委官员组成。
    - **职责**：所有外部调用请求必须经过委员会就“使用目的”、“最小必要原则”、“算法合理性”进行在线审核。
    - **机制**：一票否决权，确保每项任务的开展都具备伦理基础。
2. **“可用不可见”技术屏障**：
    - **隐私计算沙箱**：计算在可信执行环境（TEE）中进行，管理员也无法窥探原始数据。
    - **动态脱敏引擎**：根据委员会签署的授权级别，系统自动决定输出结果的粒度（如：仅输出统计均值，而非个体列表）。

2.3 价值化数据输出 (Output)

- **科研模型输出**：输出的是模型参数或分析报告，而非明文数据。
- **API 接口输出**：针对商保核赔等高频业务，仅返回“是/否”或特定指标的验证结果。

---

3. 安全委员会审批流程演示



---

4. 总结

健康数据中心不再是一个简单的“仓库”，而是一个受“数据安全委员会”监督的、基于物理隔离和隐私计算技术的“智能工厂”。这种架构确保了：

1. **输入端**：全面且标准。
2. **控制端**：流程合规且技术闭环。
3. **输出端**：价值最大化且零隐私泄露。