Механизмы приема для масштабируемого сотрудничества в области федеративных медицинских данных: проектирование и исследование доказательства концепции

Источник: JMIR Medical Informatics

Оригинал: https://medinform.jmir.org/2026/1/e89685

безопасность данных | диагностика | исследование | онкология | патология | федеративное обучение

Введение

Многие инициативы в области цифрового здравоохранения и искусственного интеллекта (ИИ) демонстрируют многообещающие результаты на пилотных этапах, но не переходят на стадию устойчивого функционирования в качестве полноценных сервисов. Пилотные проекты могут функционировать в рамках заранее определенной модели сотрудничества, тогда как операционные сервисы должны адаптироваться к изменениям в участвующих организациях, доступных ресурсах и аналитических возможностях, сохраняя при этом установленные механизмы управления и технические решения.

Цель

Настоящее исследование рассматривает переход от пилотного проекта к операционному сервису как проблему эволюции управляемой федерации и оценивает возможность платформы Open Health принимать новые формы участия, сохраняя при этом ограниченные возможности, организационный суверенитет и возможность аудита решений.

Методы

Платформа Open Health применяет модель федеративных вычислений (FC) как модель управления, отделенную от среды выполнения аналитических задач. Контекст управляемой федерации формируется до начала выполнения задач: участники получают возможности, привязанные к их держателям (holder-bound capabilities), а шлюз приема формирует явные решения «РАЗРЕШИТЬ» (ALLOW) или «ЗАПРЕТИТЬ» (DENY) до начала выполнения запрошенных операций. Доказательство концепции использует фреймворк федеративного обучения Flower и набор данных Pathology Modified National Institute of Standards and Technology (PathMNIST) из коллекции MedMNIST. Изначальная федерация состояла из больниц A и B.

Режим 1A вводит больницу C в качестве спонсируемого участника, которому разрешено отправлять локально вычисленные обновления для обучения, но запрещено использовать полученную федеративную модель для вывода (инференса). Режим 1B рассматривает ограниченное участие агентов ИИ, где ограниченные результаты могут быть преобразованы через операции, разрешенные политикой, в производные данные, потребление которых регулируется независимо от источника. Оценка проводилась по соответствию критериям приема, наличию подписанных доказательств решений, аналитическому эффекту дополнительного вклада и накладным расходам на прием.

Результаты

Демонстрационная система приняла валидные операции участников и спонсируемый вклад больницы C (режим 1A), одновременно запретив потребление модели вне возможностей больницы C, нарушения области действия (scope violations), несоответствие привязки держателю и несоответствие границам федерации. Режим 1B расширил тот же шаблон ограниченного управления на участие агентов ИИ, приняв ограниченный инференс и управляемое преобразование, но запретив несанкционированное потребление источника и привилегированный доступ к управлению.

При сопоставимых условиях обучения макро-полнота (recall) по раковым классам увеличилась с 50,2% в контрольной группе A+B до 67,4% в группе A+B+C (+17,2 процентных пункта), тогда как макро-полнота по нерецидивирующим (нелюбозным) классам изменилась с 85,5% до 86,3% (+0,8 процентных пункта). Полнота увеличилась с 19,5% до 39,9% для рака-ассоциированной стромы и с 80,9% до 94,9% для эпителия колоректальной аденокарциномы. Медианная (межквартильный размах, IQR) полная

задержка приема составила 1,210 (1,141–1,333) мс для решений «РАЗРЕШИТЬ», 1,195 (1,136–1,273) мс для решений «ЗАПРЕТИТЬ» по причине нарушения области действия возможностей и 0,884 (0,837–0,921) мс для решений «ЗАПРЕТИТЬ» по причине несоответствия привязки держателю. Каждый оцененный запрос сгенерировал подписанное доказательство решения, фиксирующее решение, причину, привязки участника и запроса, контекст управления и связанное выполнение модели.

Выводы

Платформа Open Health демонстрирует, как федеративное сотрудничество в области медицинских данных может развиваться через дифференцированное участие, сохраняя границы членства и отношения ограниченных возможностей. Основной вклад заключается в создании исполняемой границы управления, которая сохраняет отношения возможностей и производит независимо проверяемые доказательства решений, отделенные от среды выполнения федеративного обучения. Аналитический эксперимент показал, что управляемый прием дополнительного участника оказал измеримое влияние на целевые раковые классы, сохранив при этом показатели по нерецидивирующим классам. Доказательство концепции устанавливает поведение управления в контролируемых условиях; клиническая эффективность и производительность в масштабах производства требуют дальнейшей оценки.

Перевод выполнен: 04.11.2026 | ai4med.ru

Машинный перевод. Рекомендуем сверять с оригиналом при клиническом использовании.