

Лидеры по защите конфиденциальности в здравоохранении используют ИИ для улучшения мониторинга и расследования утечек данных

Источник: Bluesight

Автор: null

Дата публикации: 2025-10-01

Оригинал: <https://medcitynews.com/2026/10/healthcare-privacy-leaders-look-to-ai-to-improve-monitoring-and-data-breach-investigations/>

ENR

агентный ИИ

защита данных

кибербезопасность

управление рисками

Команды по обеспечению конфиденциальности в сфере здравоохранения все чаще используют искусственный интеллект для автоматизации процессов выявления, приоритизации и расследования потенциальных нарушений конфиденциальности. Хотя новые технологии обеспечивают более быстрый и зачастую более глубокий подход к безопасности данных, они также создают новые риски и переменные, которыми медицинские организации должны управлять, заявили лидеры в области конфиденциальности на симпозиуме по вопросам конфиденциальности, состоявшемся в среду.

Мустафа Рахими, главный стратег по искусственному интеллекту и технический лидер направления здравоохранения и наук о жизни в AWS, выступил с ключевым докладом, подводя итог центральной темы вебинара.

Где развертывание искусственного интеллекта принесет наибольшую пользу страховщикам?

Мы изучаем, как медицинские страховщики используют искусственный интеллект, определяют успех и управляют рисками кибербезопасности. Поделитесь своим мнением, заполнив наш краткий анонимный опрос.

Рахими сказал: «Доверие создает пространство для того, что действительно важно, и именно поэтому мы все здесь».

Симпозиум по конфиденциальности пациентов был организован компанией Bluesight, технологической компанией в сфере здравоохранения со штаб-квартирой в Александрии, штат Вирджиния, которая разрабатывает программное обеспечение для обеспечения соответствия требованиям больниц.

Медицинские организации переходят от реактивных аудитов конфиденциальности, как это делалось в прошлом, к программам мониторинга, которые применяют проактивный подход для выявления подозрительной деятельности и потенциальных рисков до того, как они приведут к инцидентам, связанным с конфиденциальностью данных.

Рахими представил доклад о том, что он назвал «уравнением доверия» в агентном искусственном интеллекте для здравоохранения. Его презентация исследовала, что необходимо медицинским организациям для формирования доверия к программам агентного искусственного интеллекта при их развертывании в масштабах всей организации, а именно: идентификацию агента, надежные защитные механизмы (guardrails), прозрачность и возможность проверки результатов работы агента.

«Вам нужна прозрачность, чтобы вы могли видеть, что происходит с агентом, как он мыслит», — сказал он.

Другие спикеры подчеркнули, что большой объем мониторинга не обязательно означает более качественный мониторинг. Организациям необходимо знать, являются ли данные надежными и проверяют ли они правильную деятельность для точного мониторинга рисков конфиденциальности.

Анджела Алтон, главный офицер по конфиденциальности в City of Hope — центре лечения и исследований рака со штаб-квартирой в Дуарте, штат Калифорния, — обсудила, как ее учреждение использует мониторинг доступа к электронной медицинской карте (EHR) для поддержки соблюдения требований и улучшения показателей деятельности. Она выделила случаи,

когда сотрудники получали доступ к своим собственным медицинским записям или записям близких родственников, а в нескольких ситуациях даже изменяли медицинские записи или назначали себе лекарства.

Касательно этих случаев она сказала: «Это может казаться незначительным, но это может иметь очень серьезные последствия в виде мошенничества, расточительства и злоупотреблений».

Более строгий мониторинг данных может помочь минимизировать такие случаи.

Серьезность дискуссий о безопасности данных пациентов растет. В отчете Bluesight, опубликованном в 2025 году, stated:

«В 2024 году отрасль здравоохранения пережила тревожный всплеск утечек данных, в результате которых было скомпрометировано более 300 миллионов медицинских записей пациентов — это на 26% больше, чем в 2023 году».

Искусственный интеллект сам по себе стал основным фокусом симпозиума — хотя это мощный инструмент для операций по обеспечению конфиденциальности, он сам может представлять потенциальный риск для конфиденциальности. По мере того как системы искусственного интеллекта берут на себя больше задач в рабочем процессе здравоохранения, организациям необходимо внимательно следить за тем, к каким данным они имеют доступ и какие действия они могут выполнять.

Обсуждения на симпозиуме отражают более широкую проблему для команд по обеспечению конфиденциальности в здравоохранении: по мере внедрения все более сложных технологий организации должны работать над выявлением рисков и обеспечением наличия достаточных мер контроля, уделяя особое внимание человеческому надзору, нюансированному и специфичному для каждого случая расследованию и подотчетности.

Фото: JuSun, Getty Images

Перевод выполнен: 04.10.2026 | ai4med.ru

Машинный перевод. Рекомендуем сверять с оригиналом при клиническом использовании.