ЭКОНОМИКА

Доступ к медицинским данным: обработка данных в медицинской отрасли

АНАЛИТИЧЕСКИЙ ОТЧЕТ

НОЯБРЬ 2022

ЭКОНОМИКА

Доступ к медицинским данным: обработка данных в медицинской отрасли

© 2022. АНО «Цифровая экономика». Все права защищены. Запрещается воспроизводить или передавать какую-либо часть настоящей публикации в какой бы то ни было форме какими-либо способами, включая фотокопирование и запись, или с помощью какой-либо информационно-поисковой системы.

Содержание

4 Вступительное слово

5 Введение

7 Эволюция цифровой медицины: что было и куда движемся?

11 **I. Данные в цифровой медицине**

12 Что такое большие массивы данных и зачем они нужны в медицине?

17 Цифровизация медицины, каким образом накапливаются медицинские данные?

21 Сбор данных из носимых устройств для проведения медицинской диагностики

25 **II. Основные правовые барьеры для цифровизации медицины: постановка «диагноза»**

26 Проблема: большие массивы данных есть, а доступа к ним нет

28 Регуляторные барьеры в России

45 **III. Преодоление правовых барьеров в области обработки данных в медицине: «лечение» коллизий в законодательстве**

46 Обработка данных с использованием систем ИИ в медицине: согласию быть?

50 Качественные методы обезличивания персональных данных: количество переходящее в качество?

52 Валидация больших массивов данных: можно ли использовать все данные или необходим их обязательный отбор?

58 Практическице примеры внедрения технологий искусственного интеллекта в медицине: экспериментальные правовые режимы

69 Выводы

71 Авторы и редакционная коллегия

72 Примечания

Вступительное слово

Настоящий аналитический отчет является частью серии опубликованных докладов **(«Изменение подходов к обороту персональных данных: переосмысление согласия на обработку», «Дата-посредники: организации по управлению персональными данными»)** в данном отчете авторы докладов предлагают рассмотреть новые идеи регулирования оборота медицинских данных.

Аналитическая работа, проведенная в рамках настоящего отчета, показывает необходимость решения ряда правовых и технических вопросов, чтобы гарантировать максимально эффективное использование медицинских данных в основном для достижения трех взаимосвязанных целей:

- использования медицинских данных для поддержки безопасного и эффективного функционирования системы здравоохранения, в том числе при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений) (например, при постановке диагноза и выборе подходящего лечения, предоставив врачу «второе мнение»);

- использования данных для проведения медицинских исследований и развития технологий в области ИИ (например, при разработке и тестировании новых лекарств);

- использования данных для формирования комплексной оценки методов диагностики, лекарственного и нелекарственного лечения, профилактики и реабилитации (например, обработка данных реальной клинической практики).

Снятие регуляторных барьеров призвано сделать обмен обезличенными медицинскими данными основой для развития инноваций в области ИИ за счет совершенствования правил их оборота, вовлечения доверенной третьей стороны в процесс работы с данными и упрощения процесса управления согласиями на обработку данных.

Введение

В наши дни пользователи генерируют данные регулярно: когда они открывают какое-либо приложение, ищут информацию в поисковой системе, совершают покупки в интернете или просто путешествуют со смартфоном в кармане. В результате возникают огромные массивы ценной информации, которую компании собирают, анализируют и визуализируют. Сейчас наблюдается взрывной рост объемов мировой информации, освоить их помогут новые инструменты и более развитые технологии.

За последние два десятилетия большие массивы данных стали предметом особого интереса из-за своего быстрорастущего потенциала. Однако важно не само появление больших массивов данных, как социально-экономического феномена, а то, что организации могут получить из них ценные сведения, приносящие им и обществу пользу. В частности, большие массивы данных могут быть проанализированы для получения информации, которая поможет в принятии более эффективных решений. Например, различные субъекты государственного и частного секторов генерируют, хранят и анализируют большие массивы данных с целью улучшения предоставляемых ими услуг (например, предварительно оценив привлекательность товаров и услуг, спрогнозировать спрос на рынке и реакцию на рекламную кампанию).

Подробнее со взглядом российских и международных экспертов в отношении ценности больших массивов данных можно ознакомиться в подготовленных АНО «Цифровая экономика» аналитических отчетах «Изменение подходов к обороту персональных данных» и «Дата-посредники: организации по управлению персональными данными».

В сфере здравоохранения различные типы больших массивов данных включают в себя сведения из медицинских карт пациентов, результаты медицинских осмотров и данные с устройств, являющихся частью интернета вещей, в том числе носимых устройств. Такие медицинские данные нуждаются в обработке и аналитике с помощью высокопроизводительных вычислительных решений (например, системы искусственного интеллекта). Результат такой обработки медицинских данных используется для принятия стратегически важных решений (например, для определения эффективности лекарственного средства или медицинского изделия или постановки диагноза). В противном случае поиск решения путем анализа больших объемов данных становится сравнимым с поиском иголки в стоге сена.

Однако на практике ученые, исследователи и разработчики не имеют доступа к медицинским данным, в том числе из единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ), для формирования аналитики и развития систем, основанных на искусственном интеллекте. Поэтому, для того чтобы у разработчиков была возможность создать полезные для общества системы искусственного интеллекта, необходимо решить множество правовых вопросов, связанных с доступом к таким данным и порядком их обработки.

Эффективное управление, анализ и обработка больших массивов данных могут изменить правила игры, открыв новые возможности для современного здравоохранения. Именно поэтому в различных отраслях, в том числе в здравоохранении, предпринимают активные шаги для преобразования потенциала больших массивов данных в аналитику с целью оказания более качественных услуг. Благодаря тесной интеграции биомедицинских и медицинских данных медицинские учреждения, возможно, смогут произвести революцию в оказании медицинских услуг.

Эволюция цифровой медицины: что было и куда движемся?

В настоящее время более 57% населения мира подключено к сети, доступ к которой они получают через различные технологии, включая носимые устройства, смартфоны, компьютеры и планшеты[1]. Появление и доступность интернета и новых технологий позволили гражданам свободно обмениваться информацией друг с другом в любой точке мира. Стало возможно не только «по звонку» узнавать примерный план лечения, но и проконсультироваться с врачом по видео-конференц-связи. Так, люди стали обращаться за медицинской помощью неформально и дистанционно. Такая консультация является неформальной, поскольку по телефону либо интернету в настоящее время можно получить только консультацию врача, который может собрать жалобы пациента и составить анамнез, однако окончательный диагноз можно получить только при очном посещении врача (согласно статье 36.2 Федерального закона № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»).

После появления первых и последующих побед машинного интеллекта над человеческим во все более сложных играх (от шахмат до го) появились первые проекты по использованию искусственного интеллекта, так называемые, медицинские помощники врачей (например, Botkin.ai, Celsus). Технологии его применения меняют подходы к оказанию медицинской помощи. К примеру, сегодня на основе нейронных сетей разработаны технологии в сфере медицины, и некоторые из них уже активно применяются в больницах по всему миру (например, Департамент здравоохранения Москвы совместно с ДИТ Москвы реализует городской эксперимент по использованию технологий искусственного интеллекта (ИИ) для анализа медицинских изображений). Достаточно взглянуть на 318 000 медицинских приложений на мировом потребительском рынке, чтобы понять, насколько быстро эволюционирует цифровое здравоохранение, включая телемедицину и медицинские помощники[2].

При этом потребность граждан в цифровом здравоохранении возникла тогда, когда компьютеры стали доступны почти каждому. Личный компьютер или доступ в сеть трансформировали образ потребителя различных услуг, причем не только медицинских. Сейчас граждане подбирают услуги, исходя из своего образа жизни, а не наоборот. Поэтому «удобство» цифровизации проявляется везде: в быту, промышленности, на работе, в государственном секторе. **Появляется новая модель взаимоотношений пациента и врача – модель, ориентированная на образ жизни пациента, а не наоборот.**

Ярким примером цифровизации, которая изменила подход в отношениях клиента и исполнителя, является мобильный банкинг, который позволяет без посещения банка осуществлять перевод, оплачивать коммунальные услуги и кредитную задолженность и , конечно, отслеживать все банковские операции по своим счетам за любой промежуток времени. Сегодня интернет-банкинг прочно вошел в нашу жизнь, превратившись из экзотической системы в обыденный инструмент для ежедневной работы. Теперь клиент, выбирая банк, оценивает не только условия предлагаемых продуктов, но и привлекательность, функциональность его систем дистанционного доступа.

Новые ожидания потребителя. Такая цифровизация повседневной жизни потребителя сигнализирует о возникновении новых ожиданий пациента и требований к системе здравоохранения. Люди привыкли к цифровому миру в других отраслях экономики, поэтому с появлением новых технологий потребность в цифровом здравоохранении только усиливается.

Основные драйверы цифровой медицины. Безусловно, существует несколько предпосылок развития цифровой медицины, которые сыграли свою роль одновременно. Во-первых, развитие электронной вычислительной техники.

Возможность хранить, обрабатывать, передавать терабайты данных раньше была доступна только крупным компаниям. Во-вторых, появился краудсорсинг – дешевый способ формирования огромных обучающих выборок усилиями большого числа людей через интернет. В-третьих, появилась (пусть и ограниченная на сегодняшний день) возможность собирать медицинские данные из различных источников и подпитывать алгоритмы этими данными для формирования полезной для принятия решений в области медицины аналитики. При том, что сегодня аналитика – это важный ресурс цифрового (и нецифрового) здравоохранения, способный преобразовывать данные в знания, идеи для помощи исследователям, ученым, врачам при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений).

Потенциальный драйвер цифровой медицины. При этом эксперты особо подчеркивают важность разработок программного обеспечения по обезличиванию персональных данных. Предоставление такого программного обеспечения и методик обезличивания само по себе решает многие задачи и проблемы медицинской организации, существующие на сегодняшний день, и является еще одним потенциальным инструментом для развития цифровой медицины.

Барьеры для развития цифровой медицины все еще существуют. Расширенное использование искусственного интеллекта в здравоохранении все еще затрагивает большое количество вопросов, связанных с доступом к медицинским данным и оборотом персональных и обезличенных данных. Такие вопросы вызваны наличием пробелов и неопределенностей в правовом регулировании, что может привести к тому, что такая социально значимая сфера, как медицина, не получит пользу от существующих на сегодняшний день возможностей в сфере инноваций (подробнее в главе 2).

1970–2000	2000–2020	2020+
ИТ в области здравоохранения	**Электронное здравоохранение**	**Цифровое здравоохранение**
Появление медицинской информатики (исследование процессов получения, передачи, обработки, хранения, распространения, представления информации с использованием информационной техники и технологии в медицине и здравоохранении) как дисциплины.	Рост показателей хронических заболеваний вызвал потребность в анализе больших массивов данных.	Появление разработок в сфере ИИ, робототехнике, машинного обучения, интернета вещей, приложения для здоровья, виртуальной и дополненной реальности.
Внедрение проблемно-ориентированной медицинской информационной системы, которая позволяет получать доступ к медицинской карте с большим объемом информации.	Потребность в электронном здравоохранении возникает в связи с активным использованием персональных компьютеров и доступом к информации через интернет.	Широкое распространение использования ИКТ в «цифровых» обществах.

Появление персональных компьютеров на рынке потребителей.	В 2008 г. опубликовано поручение Президента России о создании и развитии государственной информационной системы персонифицированного учета оказания медицинской помощи гражданам России, а Министерство здравоохранения и социального развития Российской Федерации выпустило приказ «Об утверждении концепции создания единой государственной информационной системы в сфере здравоохранения».	Потребность граждан в медицинских услугах в электронной форме.
Появление ИТ-отделений в больницах (в соответствии с рекомендациями Совета Министров СССР в больницах начали создавать отделы автоматизированных систем управления).	Постановление Правительства Российской Федерации № 555 от 05.05.2018 (утратило силу) устанавливает порядок по предоставлению данных в ЕГИСЗ. Требования действуют для всех негосударственных медицинских организаций, в том числе частных клиник и медицинских центров, с 1 января 2019 года. С 1 января 2020 года медицинские справки и заключения в России стали выдаваться в электронном виде наряду с бумажными носителями. В феврале 2022 года опубликовано Постановление Правительства России № 140 от 9 февраля 2022 г. «О единой государственной информационной системе в сфере здравоохранения», которое описывает продолжение работы всех участников процесса по развитию цифрового контура в здравоохранении.	
Фокус		
Совершенствование логистики и организационных функций медицинских учреждений, а также повышение эффективности в области здравоохранения.	Улучшение качества оказания медицинской помощи посредством использования информационных систем.	Улучшение качества оказания медицинских услуг – ориентированность на потребителя, соответствие его образу жизни. Создание условий для сбора данных из новых источников данных (например, носимые устройства, датчики, данные социальных сетей).

I. Данные в цифровой медицине

1. Что такое большие массивы данных и зачем они нужны в медицине?

Термин «большие массивы данных» можно описать как структурированные и неструктурированные данные, генерируемые из множества источников в огромном объеме и с большой скоростью в режиме реального времени[3]. Такие данные становятся важными, когда связанный с ними анализ приводит к более эффективному принятию решений.

Рост объема больших массивов данных в здравоохранении происходит в ответ на оцифровку медицинской информации, что побуждает представителей медицинской отрасли использовать аналитику данных, например, при разработке лекарственных препаратов, при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений), контроле за хроническим состоянием пациентов.

Международный опыт

Пользуясь возможностями анализа больших массивов данных, технологические компании создают интеллектуальные продукты и сервисы, способные решать принципиально новые задачи для медицины. Например, в США разработали систему «вычислительной биологии», которая позволяет видеть взаимодействие химических веществ с сигнальными рецепторами клеток организма[4]. С помощью обработки больших массивов данных, возможно, удастся произвести настоящую революцию в фармакологии: обработка больших массивов данных может помочь в создании лекарственных препаратов, способных точно попадать в цель, а значит, оптимально подходящих для лечения тех или иных заболеваний.

При этом важно понимать, что значение для аналитики имеют не только медицинские данные, которые позволяют сделать заключения о здоровье человека (например, анализы биологических показателей, нейрофизиологические данные, геномные данные), но и данные, которые могут оказать влияние на здоровье человека (данные с носимых устройств, например режим сна пользователя).

Следует отметить, что для формирования правового регулирования необходимо сначала определиться с тем, **зачем нужны большие массивы данных в медицине и существует ли запрос разработчиков** на снятие существующих регуляторных барьеров. Возможно, имеет смысл расставить приоритеты и предусмотреть особенности в тех сферах правового регулирования в области здравоохранения, которые кажутся для рынка наиболее востребованными.

Международный опыт

Например, в Великобритании в октябре 2019 года были созданы Центры исследования медицинских данных с целью создания единой точки доступа к наборам медицинских данных в строго определенных сферах здравоохранения[5], в частности: проведение клинических испытаний, прогнозирование рисков возникновения психических расстройств, лечение рака, воспалительных заболеваний кишечника, медицинская диагностика (при наличии согласия пациента), офтальмология, исследования в области легких и сердечно-сосудистой системы, а также медицинская помощь, оказываемая в рамках клинической

апробации. Через полтора года функционирования благодаря Центру исследования медицинских данных было запущено 300 проектов в области обработки медицинских данных[6].

Ниже приведены примеры сфер применения больших массивов данных в медицине.

Данные для поддержки принятия врачебных решений

ИИ может использоваться для получения «второго мнения» при постановке диагноза. ИИ дает возможность быстрее анализировать медицинские изображения (рентгеновские снимки, КТ, МРТ, маммограммы, макроснимки гистологических препаратов и пр.), выявляя возможные патологии и сигнализируя о них. Таким образом, сокращается время на постановку диагноза, которое может быть критично для пациента, снижается количество ошибок и уменьшается стоимость обследования.

При этом отметим, для того чтобы системы на базе ИИ могли самостоятельно, независимо от врача, принимать решения, а не быть только лишь поддержкой при принятии решений («вторым мнением»), существует ряд проблем, связанных с неоднозначным правовым режимом ответственности при эксплуатации ИИ, а также с регуляторными барьерами, препятствующими искусственному интеллекту «получить больше опыта и знаний».

Примеры

Сейчас разработчики медицинских сервисов на основе искусственного интеллекта имеют доступ к наборам данных, которые охватывают большинство основных исследований: УЗИ, ЭКГ, КТ, МРТ, рентгенографию и другие. С помощью наборов данных разработчики и исследователи смогут обучить собственные модели находить патологии на медицинских снимках.

В настоящее время наиболее популярными являются наборы данных КТ-изображений органов грудной клетки для обучения ИИ-сервисов поиску признаков COVID-19. На втором месте – объединенные наборы данных по нескольким видам исследований, таким как КТ, маммография, рентгенография и флюорография. На третьем – набор данных МРТ головного мозга. Большая часть наборов применяется для калибровочных, функциональных и других видов тестирований ИИ-сервисов[7].

Такие технологические решения позволяют радиологам или кардиологам выявлять важные данные для определения приоритетности критических случаев, избегать потенциальных ошибок при чтении электронных медицинских карт (EHRS) и устанавливать более точные диагнозы. Алгоритмы искусственного интеллекта могут анализировать эти наборы данных с высокой скоростью и сравнивать их с другими исследованиями, чтобы выявить закономерности и скрытые взаимосвязи при наблюдении за пациентом. Этот процесс позволяет специалистам быстро отслеживать важную для постановки диагноза информацию.

Например, в начале мая 2019 года IBM выпустила программное обеспечение Watson Imaging Patient Synopsis для анализа анамнестических данных пациентов. Данное ПО призвано помочь специалистам по МРТ и КТ. ПО уже протестировано и используется рентгенологами медицинского центра Hardin Memorial Health. Технология IBM, которая называется The Patient Synopsis, уникальна тем, что ранее ИИ никогда не использовался для расшифровки и обработки неструктурированных данных из амбулаторных карт[8].

Технология Patient Synopsis позволяет проанализировать информацию о диагностических и медицинских процедурах, результатах лабораторных исследований, истории болезни и существующих аллергических реакциях у пациента, а также предоставляет рентгенологам и кардиологам краткое изложение, в котором основное внимание уделяется содержанию медицинских изображений.

Обработка неструктурированных данных

В 2020 году медицинские информационные системы внедрили 82% медицинских организаций России. И хотя 80% информации в электронных медицинских картах хранится в неструктурированном виде, с ней можно работать с помощью технологий обработки текста на естественном языке (Natural Language Processing, NLP). ИИ может искать, собирать, хранить и стандартизировать медицинские данные независимо от формата, помогая выполнять повторяющиеся задачи при принятии решений о диагностике и лечении пациентов.

Проект Amazon HealthLake

Облачное подразделение Amazon выпустило новый инструмент, облегчающий организациям здравоохранения поиск и анализ данных. Так, компания Amazon Web Services в декабре 2020 года представила инструмент Amazon HealthLake, при помощи которого пользователи могут собирать, искать и анализировать данные для более точного прогнозирования состояния здоровья пациентов и населения[9].

Amazon HealthLake – это сервис, соответствующий требованиям Закона о преемственности и подотчетности медицинского страхования США (англ. Health Insurance Portability and Accountability Act, HIPAA), который предлагает компаниям, работающим в сфере здравоохранения и медико-биологических наук, доступ к наборам данных о здоровье отдельного человека или группы пациентов. Цифровой сервис Amazon HealthLake объединяет данные из хранилищ различных организаций в централизованное озеро данных Amazon Web Services (AWS) и автоматически валидирует собранную информацию с помощью машинного обучения.

Прогнозная аналитика

Прогнозная аналитика позволяет автоматически анализировать медицинские данные, выявлять факторы риска и подозрения на заболевания, формировать на их основе прогнозы, содержащие комплексную оценку вероятности развития различных заболеваний, потребности в лекарственных препаратах, предупреждения распространения эпидемии, точный индивидуальный прогноз ухудшения самочувствия пациента.

По сути, хронические заболевания можно прогнозировать и отслеживать скорость их прогрессирования. CloudMedX[10] – это компания, которая специализируется на декодировании неструктурированных данных, хранящихся в виде заметок (заметки врача, выписки, заметки о диагнозе и госпитализации и т. д.).

Эти заметки используются в качестве источника для получения клинической информации медицинскими сотрудниками, помогая принимать основанные на этих данных решения для улучшения результатов лечения пациентов. Решения CloudMedX[11] уже применяются при составлении плана лечения нескольких видов заболеваний, таких как почечная недостаточность, пневмония, застойная сердечная недостаточность, гипертония, рак печени, диабет и инсульт, с заявленной целью

снизить затраты для пациентов и врачей за счет оказания помощи в ранней и точной диагностике пациентов[12].

Обработка и анализ данных с носимых устройств

Носимые устройства (фитнес-браслеты, умные часы), позволяющие отслеживать артериальное давление, частоту сердцебиения, уровень сахара в крови, могут помочь в сборе данных для мониторинга заболеваний и послеоперационных осложнений (например, для дистанционного наблюдения пациентов с артериальной гипертензией и сахарным диабетом). Для этого необходимо создание доверенной среды оборота данных, собранных с носимых устройств, для передачи такой информации врачам и пользователям носимых устройств.

Напомним также, что 6 октября 2021 года Правительство утвердило перечень инициатив социально-экономического развития до 2030 года. В число «проектов маяков», которые реализуются в рамках перечня социально-экономического развития до 2030 года в том числе включен проект «Персональных медицинских помощников». Согласно данному проекту данные с мобильных медицинских устройств (глюкометров и других трекеров) от пациентов будут передаваться на общую платформу и связываться с электронной медицинской картой больного. Благодаря этому врач сможет отслеживать критические показатели в режиме реального времени, а система искусственного интеллекта сможет спрогнозировать ухудшение состояния здоровья человека.

Инициатива «Персональные медицинские помощники»

Инициатива «Персональные медицинские помощники» была сформулирована еще в 2021 году. В рамках данной инициативы Минздрав России намерен реализовать пилотный проект по мониторингу для создания централизованной системы динамического наблюдения за состоянием здоровья. Как отмечается в паспорте Стратегии цифровой трансформации отрасли «Здравоохранение» до 2024 года и на плановый период до 2030 года «Персональные медицинские помощники» – это проект, направленный на создание технологий для динамического наблюдения с использованием платформ централизованных диагностических сервисов на базе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ) и интеграцию платформ централизованных диагностических сервисов на базе единой государственной информационной системы в сфере здравоохранения с единым порталом государственных услуг, супер-сервисом «Мое здоровье», а также перевод функционирующего диагностического оборудования в медицинских организациях и персональное использование в цифровом формате и подключение к платформам централизованных диагностических сервисов.

Система будет интегрирована с ЕГИСЗ и основными платформами в сфере здравоохранения. Она будет обрабатывать сведения, получаемые с персональных медицинских устройств.

ИИ для диагностики психических заболеваний и расстройств

Обработка и анализ данных с использованием ИИ также особенно актуальны в психиатрии. Одной из ключевых проблем в данной отрасли является своевременное выявление психических расстройств и заболеваний[13]. По данным экспертов, службы первичной медико-санитарной помощи способны выявить только 50% случаев депрессии у пациентов. Такая же проблема существует и при выявлении суицидального поведения[14]. В тематических исследованиях отмечается, что службы первичной медико-санитарной помощи не способны выявить порядка 60–70% случаев суицидального поведения[15].

С целью повышения точности выявления и диагностики психических расстройств необходимо проанализировать широкий объем информации: особенности когнитивных функций пациента, закономерности его поведения[16]. Однако в настоящее время основным источником такой информации является сеанс (интервью) врача с пациентом, а также отчеты самого пациента[17]. Для совершенствования диагностики и выявления психических расстройств и заболеваний профессор Лян в 2019 году предложил использовать следующие источники данных о психическом здоровье: данные, собранные из мобильных и носимых устройств, социальных сетей, электронных медицинских карт, записей о приеме лекарств и иные данные, в том числе неструктурированные записи[18].

Аналитика больших массивов данных и искусственный интеллект открывают возможности для преодоления существующих проблем в выявлении и диагностике психических расстройств и заболеваний. Например, обработка данных, разрешенных для распространения в социальных сетях, может помочь выявить проблемы с психическим здоровьем у пользователей, которые, возможно, не желают раскрывать свои чувства психиатрам и врачам, но готовы поделиться в социальных сетях (или, например, если пользователь отметил лайком «опасный» контент).

Так, методология обработки естественного языка (NLP) и машинного обучения (ML) создает возможности для выявления психических расстройств на основе данных, собранных в социальных сетях (данные, собранные из контента, который люди публикуют публично). Методы NLP позволяют извлечь из написанного текста в социальных сетях несколько характеристик, включая характеристику личности, демографические данные и психический статус/диагноз. Анализ настроений является одним из популярных инструментов для извлечения сведений в социальных сетях и применяется для понимания эмоционального состояния пользователя. Помимо анализа настроений, другие подходы к извлечению признаков психических расстройств включают лингвистическое исследование и подсчет слов (LIWC, программа для анализа текстов). После извлечения и отбора данные передаются алгоритмам ИИ для выявления проблем с психическим здоровьем[19]. Например, в мировой практике существуют проекты, направленные на выявление депрессии несовершеннолетних пользователей путем анализа фотографии в социальной сети Instagram (запрещена в России, организация признана экстремистской)[20].

Необходимыми для выявления и диагностики психических расстройств и заболеваний могут стать также данные, собранные с помощью носимых устройств, которые широко используются для мониторинга физической активности и состояния здоровья людей, включая количество шагов, частоту сердечных сокращений, время сна. Благодаря достижениям в области больших массивов данных и методам машинного обучения, эти данные можно было бы использовать для уменьшения количества ошибок при постановке диагноза, в частности из-за сложностей, возникающих при обмене информацией между пациентами и практикующими врачами.

К примеру, исследователями в области больших массивов данных был запущен проект, благодаря которому по результатам обработки данных, собранных с носимых устройств, включая пульс, электродермальную активность, частоту сердечных сокращений, интервал между ударами и температуру кожи, у пациента выявлено 70% стрессовых событий с 95% точностью. В ходе этого исследования с использованием методов машинного обучения был разработан контекстно-ориентированный детектор стресса[21].

Источников больших массивов данных может быть много, и приведенные выше примеры не являются исчерпывающими, но могут, на наш взгляд, служить основой для дальнейших обсуждений.

Для этого предлагается закрепить доступ разработчиков к большим массивам данных из различных источников, включая электронные медицинские карты (в частности, к ЕГИСЗ), носимые устройства[22]. Как только данные из различных источников будут собраны и стандартизированы, искусственный интеллект будет использовать их для обработки и подготовки аналитики[23]. Как справедливо отмечают эксперты Шетти и Хатчинсон, применение больших массивов данных и искусственного интеллекта (особенно машинного обучения) позволит улучшить[24]:

1. выявление и диагностирование психического расстройства;
2. исследования эффективности лекарственной терапии, фаз протекания заболеваний[25];
3. прогнозирование риска насилия среди пациентов;
4. выявление социальной напряженности, депрессии, различных видов агрессии, деменции, аутизма и склонности к суициду.

Практические примеры применения ИИ

Институт русского языка им. В .В . Виноградова, Научный центр психологического здоровья и Психологический институт РАО запустили сервис для выявления депрессии, различных видов агрессии, деменции, аутизма и склонности к суициду по текстам, оставляемым субъектами в интернете, и данным их профилей в социальных сетях. Например, по идентификатору профиля в сети «ВКонтакте» система дает психологическую характеристику человека, включая черты его личности, конфликтность, склонность к депрессии и фрустрации и т. п.

2. Цифровизация медицины, каким образом накапливаются медицинские данные?

В международных тематических исследованиях отмечается, что построение безопасной, эффективной и устойчивой системы здравоохранения в значительной степени зависит от возможностей доступа к данных и их обработки. Аналитика данных может стать «вторым мнением» при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений).

Такие данные включают структурированные данные в электронных медицинских картах, медицинские изображения (например, КТ, МРТ), лабораторные отчеты и другие средства управления данными, используемые в системах здравоохранения. К таким данным можно также отнести те, которые собираются за рамками медицинских учреждений, в том числе с носимых устройств (например, фитнес-трекеров)[26].

Единая государственная информационная система в сфере здравоохранения (ЕГИСЗ) – это национальная информационная система, созданная для обеспечения эффективной информационной поддержки органов и организаций системы здравоохранения, а также граждан в рамках процессов управления медицинской помощью и ее непосредственного получения. Постановление Правительства Российской Федерации № 555 от 5.05.2018[27] (утратило силу) предписывало

передавать в ЕГИСЗ несколько типов данных. В первую очередь среди них: информация о самой медицинской организации и врачах, а также данные о случаях медицинского обслуживания, в том числе амбулаторные и стационарные эпикризы. Требования начали действовать для всех негосударственных медицинских организаций, в том числе частных клиник и медицинских центров, с 1 января 2019 года. Однако по факту обмен данными не осуществлялся.

Постановление Правительства Российской Федерации от 05.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения»[28] (утратило силу) подвело черту под действующей концепцией информатизации. Данный документ оставил за ЕГИСЗ только федеральный сегмент, отделив от нее информационные системы регионального уровня и уровня медицинских организаций, и сфокусировал ее на агрегации отраслевой статистики и управленческой информации. Сменившее Постановление Правительства Российской Федерации № 555 Постановление Правительства России № 140 от 9 февраля 2022 г. «О единой государственной информационной системе в сфере здравоохранения» описывает продолжение работы всех участников процесса по развитию цифрового контура в здравоохранении[29]. Также постановление расширяет функционал Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ).

Системы, призванные обеспечить обмен электронных рецептов и учет льготных лекарственных средств, внедряются на уровне регионов, т. е. в РМИС, или в так называемые государственные информационные системы (ГИС) в сфере здравоохранения субъектов Российской Федерации. Персонализированные интегрированные электронные медицинские карты (ИЭМК) ведутся и хранятся в медицинских информационных системах медицинских организаций (МИС МО), а в одноименной подсистеме ЕГИСЗ эти данные будут содержаться в обезличенном виде. Согласно Постановлению Правительства России № 140 от 9 февраля 2022 г. информационная система свяжет между собой все региональные медицинские организации. При этом большинство документов – выписки, справки и медкарты должны перейти в электронный вид. Врачи получат доступ к необходимым документам, например к истории болезни, даже если человек переезжал и менял поликлинику или больницу.

От первого лица

Борис Зингерман
Генеральный директор Ассоциации НБМЗ и руководитель направления цифровой медицины компании ИНВИТРО

Обработка медицинских данных регулировалась определенными этическими нормами задолго до появления «защиты персональных данных». При публикации медицинских исследований обязательно соблюдалась «врачебная тайна», а дополнительные меры по защите именно персональных данных за прошедшие 15 лет добавили много формальных и организационных трудностей, но, похоже, незначительно повысили их защищенность. Ценность медицинских данных всегда осознавалась врачами и учеными и часто порождала конкуренцию в части их использования в научных работах и диссертациях. Сейчас же на фоне успехов искусственного интеллекта и машинного обучения их ценность возросла многократно. Осознание этой ценности подстегивается публикациями в СМИ типа «данные – нефть XXI века». И это осознание ценности ведет к дополнительной конкуренции владельцев данных. При этом само понятие «владельца» медицинских данных (а точнее того, кто может этими данными распоряжаться) остается очень туманным и неопределенным. Главных претендентов трое – сам пациент, медорганизация и государственные информационные системы (у нас – ЕГИСЗ и Региональные МИС). Традиционно основным распорядителем данных была медицинская организация, которая их выявляла и фиксировала. Сейчас акценты все больше смещаются в сторону самого пациента, особенно в ситуациях,

когда необходим обмен данными между разными медорганизациями. Постановление Правительства №555 «О единой государственной информационной системе в здравоохранении (ЕГИСЗ)» четко фиксировало, что передача медицинских данных из одной медорганизации в другую осуществляется только с согласия пациента, однако никаких механизмов предоставления такого согласия предусмотрено не было. В пришедшем ему на смену в 2022 году новом Постановлении Правительства №140 в ЕГИСЗ заявлен (и уже реализован) механизм, с помощью которого пациент может сам загрузить и предоставить другому врачу или медорганизации свои медицинские данные. Учитывая, что все прочие медицинские данные хранятся в ЕГИСЗ в обезличенном виде, получение датасетов, объединяющих данные из различных медицинских организаций, требует явного участия пациентов. Именно поэтому наша Ассоциация уже в течение 3-х лет пытается инициировать создание специальных сервисов, которые позволили бы пациентам собирать свои медицинские данные, а также делиться ими с заинтересованными научными или коммерческим организациями. Такой механизм представляется очень перспективным и соответствующим современным трендам, но пока еще очень далек от реализации.

Следует отметить, что Минздрав России утвердил Порядок обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования (Приказ Минздрава России от 14.06.2018 № 341н). Порядок применяется в отношении обезличивания сведений, обрабатываемых в подсистеме «Федеральная интегрированная медицинская карта» ЕГИСЗ. Обезличивание сведений проводится с целью защиты сведений от несанкционированного использования с одновременным сохранением возможности их дальнейшей обработки.

Напомним, обезличиванию подлежат: фамилия и имя, пол, дата и место рождения, гражданство, паспортные данные, место жительства и регистрации, номера СНИЛС и полиса ОМС, анамнез, диагноз, вид оказанной медпомощи и ряд других сведений. Процесс обезличивания производится автоматически средствами подсистемы.

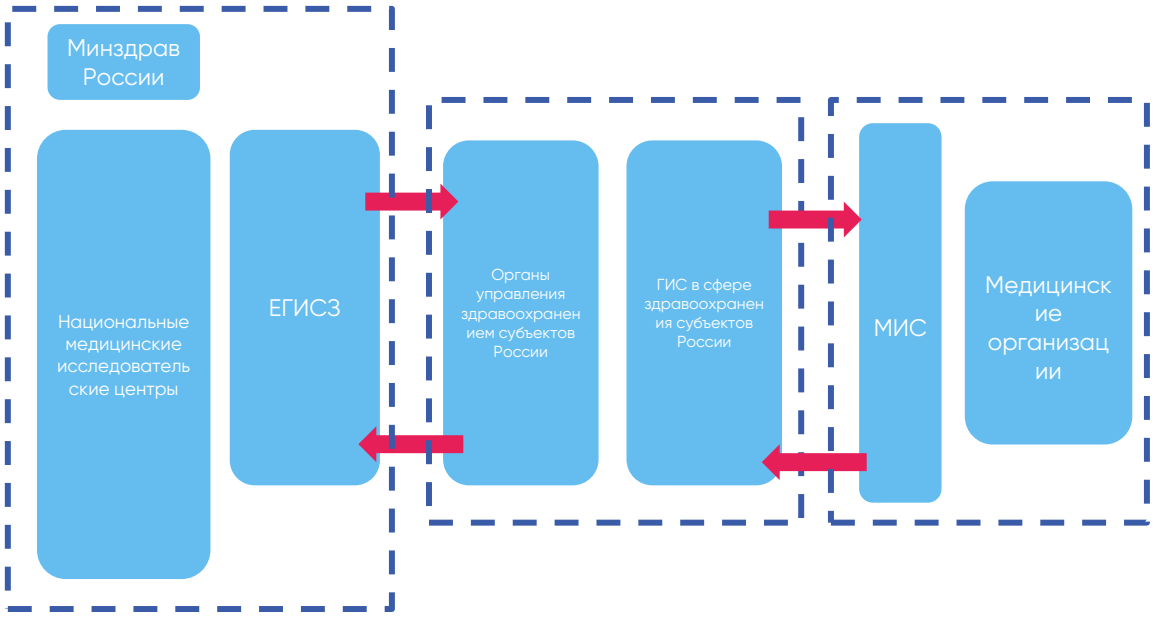
При этом в любую медицинскую информационную систему (МИС) входят такие основные блоки, как:

- электронные карты пациентов,
- показания с медицинских приборов,
- данные исследований,
- система для коммуникации между медицинскими работниками,
- финансовая и административная информация.

Следует отметить, что последние 10–15 лет МИСы постоянно расширяли свои функциональные возможности: добавлялась электронная медицинская карта, модули профилактической направленности. Сегодня они насчитывают десятки встроенных модулей, сотни окон ввода данных, тысячи функций. Постепенно увеличивается объем больших массивов данных, накапливаемых в МИС. Такие большие массивы данных необходимы для развития искусственного интеллекта в здравоохранения.

Для обмена информацией между подсистемой ИЭМК медицинской организации и внешними системами будет использоваться Регистр электронных медицинских документов (РЭМД) – подсистема, входящая в состав ЕГИСЗ.

Схема информационных систем в сфере здравоохранения



Стандартизация – один из важнейших инфраструктурных элементов права и экономики. Так, в сфере здравоохранения введены стандарты ГОСТ Р ИСО / ТС 18308-2008 «Информатизация здоровья. Требования к архитектуре электронного учета здоровья», ГОСТ Р 52978-2008 «Информатизация здоровья. Состав данных о лечебно-профилактическом учреждении для электронного обмена этими данными. Общие требования», ГОСТ Р 52976-2008 «Информатизация здоровья. Состав первичных данных медицинской статистики лечебно-профилактического учреждения для электронного обмена этими данными. Общие требования». Цель данных стандартов – установить общие требования к информационному обмену между учреждениями системы здравоохранения. Однако согласно текущему регулированию[30] стандарты не являются обязательными для применения, поскольку действует принцип добровольности применения национальных стандартов. В связи с этим чаще всего владельцы информационных систем и разработчики не следуют предписаниям национальных стандартов, поэтому возникает проблема разрозненного характера ввода и хранения данных в медицинских информационных системах.

Стандартизация является инструментом обеспечения единообразия и качества на всех уровнях управления информацией. Грамотный подход при формировании стандартов поможет решить существующие на практике технические проблемы. По этой причине представляется целесообразным рассмотреть возможность пересмотра существующей системы стандартизации в области ввода и хранения медицинских данных в информационных системах.

Также напомним, что Минздравом России выпущены методологические рекомендации по МИС МО[31] и РМИС, которые призваны обеспечить единообразие требований к информационным системам для всех участников информатизации здравоохранения: разработчиков МИС, руководителей медицинских организаций и органов управления здравоохранением, контролирующих органов. В них, в частности, указаны единые для всех требования к системам, единые критерии эффективности и уровни автоматизации медицинской организации, возможность проводить сравнения.

3. Сбор данных из носимых устройств для проведения медицинской диагностики

Сегодня достижения в области сенсоров, систем слежения и искусственного интеллекта помогают врачам диагностировать разного рода хронические заболевания путем дистанционного наблюдения за состоянием здоровья пациентов с использованием носимых устройств. Такого рода носимые устройства (например, смарт-часы, фитнес-браслеты) способны собирать, хранить и передавать данные о состоянии здоровья физических лиц в качестве дополнительного источника информации при оказании услуг по профилактике заболеваний.

По оценкам Deloitte, в 2022 году по всему миру будет выпущено более 320 миллионов носимых устройств для мониторинга здоровья и самочувствия потребителей[32]. К 2024 году этот показатель, вероятно, достигнет 440 миллионов, поскольку на рынке появятся новые разработки и все больше медицинских организаций привыкнут к их использованию[33]. В число таких носимых устройств входят как умные часы, так и носимые устройства медицинского назначения.

Согласно исследованию Deloitte за 2021 год, 39% респондентов владеют умными часами. Изначально их наиболее распространенное применение заключалось в том, чтобы помочь пользователям прийти в спортивную форму, сбросить вес и улучшить свой личный рекорд по бегу. Однако все чаще люди стали использовать умные часы для мониторинга своего здоровья, а не только для учета темпа бега. Появление нового программного обеспечения такого рода превратило их в персонализированных медицинских помощников. Мониторы сердечного ритма в настоящее время входят в стандартную комплектацию большинства умных часов, а некоторые из них одобрены агентством Министерства здравоохранения и социальных служб США (FDA) для выявления таких отклонений сердца, как фибрилляция предсердий. По мере того как эти устройства становятся все более совершенными, процент потребителей, использующих их для мониторинга хронических заболеваний и выявления симптомов серьезных заболеваний, скорее всего, будет увеличиваться.

Международный опыт

В настоящее время носимые устройства (медицинские и немедицинские изделия) подлежат надзору со стороны различных органов власти в Соединенных Штатах Америки, например предварительное одобрение для запуска на рынок и последующий надзор за медицинскими изделиями относятся к ведению FDA. Оборот немедицинских изделий контролируется Федеральной торговой комиссией.

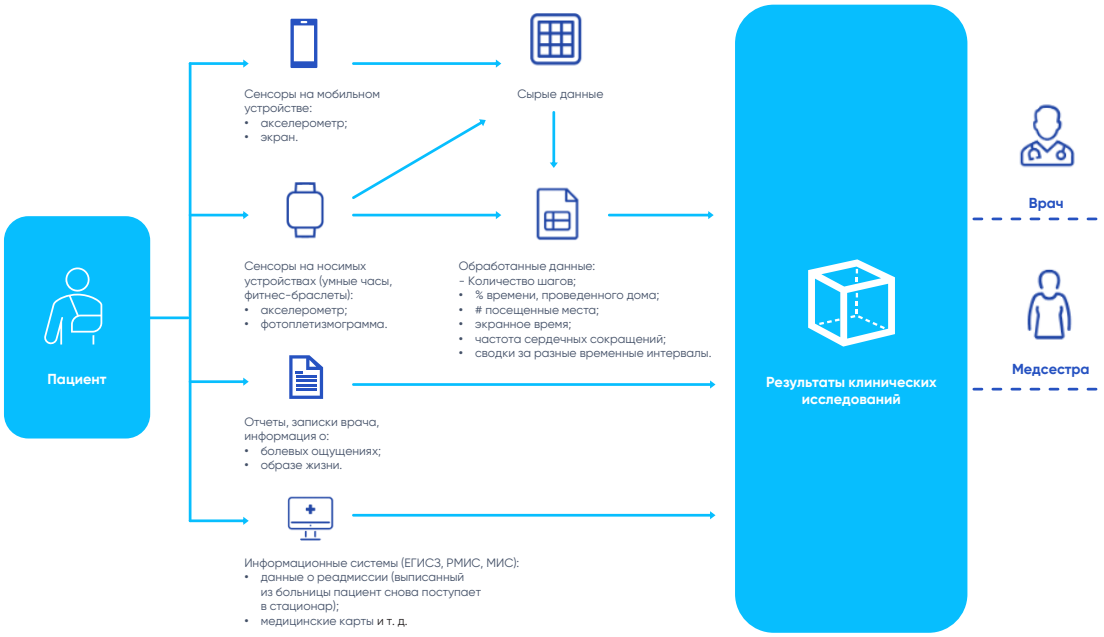
Тем не менее в обыденной жизни стирается грань использования носимых устройств медицинского и немедицинского назначения. Производители носимых устройств, такие как Apple и Fitbit, стремятся расширить линейку своей продукции до сертифицированных медицинских изделий для мониторинга здоровья и привлечь страховые компании и предприятия в качестве клиентов, в то время как производители традиционных медицинских изделий также создают устройства немедицинского назначения.

Наряду с социальными преимуществами и развитием инноваций, которые обеспечиваются обработкой данных с носимых устройств, возникают и новые вызовы, связанные с использованием данных, содержащих подробные сведения о здоровье и поведении человека.

В частности, вопросы стандартизации данных и операционной совместимости технологий представляют серьезные препятствия для объединения и извлечения пользы из разных типов данных, содержащихся в различных источниках, в целях улучшения медицинского обслуживания и достижения прогресса в исследованиях. Несмотря на то что в экосистеме здравоохранения развернуты миллионы устройств для мониторинга человеческого организма, от больничной койки до носимых устройств, преобладание закрытых способов связи приводит к отсутствию операционной совместимости между этими устройствами. Отсутствие стандартизированной платформы для получения непрерывных потоков данных с различных устройств ограничивает использование этих данных для получения ценной информации, если только все потоки данных не исходят от совместимых устройств.

Еще одной проблемой, помимо операционной совместимости, является качество данных, их точность, особенно в случае с использованием фитнес-браслетов и других носимых устройств. В настоящее время медицинские и немедицинские устройства подпадают под разные нормативные требования к медицинским изделиям. Однако по мере того как носимые устройства (фитнес-браслеты, карманный кардиолог) интегрируются в систему здравоохранения, например для мониторинга частоты сердечных сокращений и расхода энергии у пациентов с сердечно сосудистыми заболеваниями, вопрос о том, достигают ли их измерения уровня клинически приемлемой точности, требует дополнительного обсуждения.

Схема сбора медицинских данных



Международный опыт регулирования

Европейский союз[34] **и Великобритания (GDPR)**[35] Если персональные данные пользователя собираются и обрабатываются с помощью приложения носимого устройства, то законным основанием обработки любых персональных данных специальной категории является согласие субъекта персональных данных,

выраженное в явном виде. В соответствии со статьей 4(11) GDPR под согласием понимается «добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных». Также согласно статье 7(3) GDPR оператор (контролер) персональных данных обязан обеспечить, чтобы субъект данных в любой момент времени мог отозвать согласие также легко, как оно было предоставлено. Более того, оператор (контролер) персональных данных должен обеспечить защиту от дальнейшей обработки персональных данных.

Однако практика сбора данных с помощью носимых устройств не всегда вписывается в текущее регулирование GDPR. Например, если спортивное учреждение использует носимое устройство для анализа данных о спортивных достижениях профессиональных спортсменов. Между спортсменами и спортивными учреждениями существуют трудовые отношения[36]. В таком случае данное согласие на сбор и обработку данных не подпадает под критерий «добровольности» и может быть признано недействительным.

В такой ситуации законным основанием для обработки данных может быть основание, предусмотренное статьей 9(2)(b) или 9(2)(h) GDPR и GDPR Великобритании, в частности: **«обработка необходима в целях профилактической или профессиональной медицины, для оценки трудоспособности работника, для диагностики медицинского состояния, предоставления медицинской или социальной помощи или лечения или для управления системами и услугами здравоохранения и социального обеспечения на основании законодательства Союза или государства-члена или на основании договора с работником здравоохранения и в соответствии с условиями и гарантиями, указанными в параграфе 3».**

II. Основные правовые барьеры для цифровизации медицины: постановка «диагноза»

1. Проблема: большие массивы данных есть, а доступа к ним нет

Страны можно разделить на две группы: юрисдикции с консервативным регулированием обработки медицинских данных, т. е. те, которые придерживаются условно подхода «получи согласие или обезличивай» (например, Германия, Израиль), и либеральным подходом, когда согласие субъекта персональных данных при повторном использовании его данных не требуется (Финляндия). В первом случае персональные данные могут использоваться разработчиками ИИ только в том случае, если получено информированное согласие пациента или данные полностью (необратимо) обезличены[37]. Однако законодательное закрепление обязанности получить (повторное) согласие от пациента может привести к значительным административным и финансовым затратам и сложностям, которые могут значительно усложнить процесс обработки данных и вовсе сделать такую обработку невозможной[38]. Обязанность получить (повторное) согласие может также привести к серьезным искажениям при отборе данных.

В России для RWE-исследований необходимо обрабатывать большие массивы данных, а в силу пункта 1 части 1 статьи 6 и пункта 1 части 2 статьи 10 Федерального закона «О персональных данных» требуется получать письменные согласия субъектов персональных данных; необходимость получения тысяч письменных согласий является серьезным барьером. Во-первых, получить согласие бывает весьма сложно, а во-вторых, сегодня у пациента нет возможности дать такое разрешение в режиме онлайн.

В России также наибольшие сложности возникают при попытке получить доступ к данным из других организаций через единую государственную информационную систему в сфере здравоохранения (ЕГИСЗ) и региональные медицинские информационные системы (РМИС). В ЕГИСЗ накоплен огромный объем информации, которая, однако, является скорее статистической, в связи с чем не всегда подходит для работы с использованием ИИ.

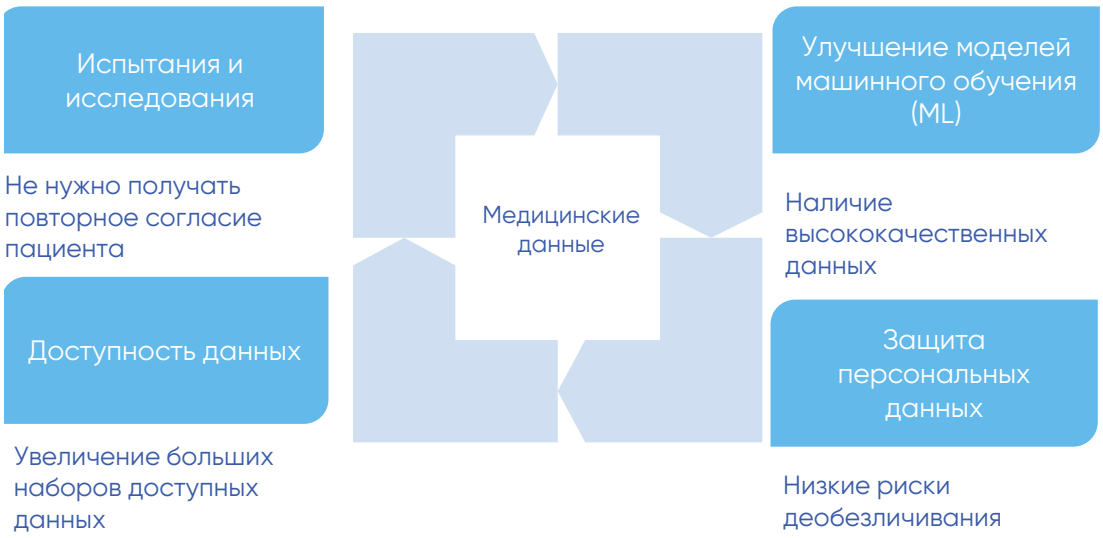
Кроме того, хотя обезличенные данные выходят за рамки Общего регламента по защите персональных данных (GDPR), анонимизация данных сопряжена с техническими и юридическими проблемами. Достижение полной анонимизации становится все более сложной задачей из-за возможности перекрестного связывания наборов данных и специальной категории данных, таких как генетические данные[39]. Также следует отметить, что полное обезличивание может включать удаление важной информации, необходимой для проведения медицинских исследований. Полное обезличивание снижает ценность и возможность анализа медицинских данных, а также эффективность и пользу аналитических отчетов, полученных на их основе. Например, основной международный тренд и успехи в обработке данных реальной клинической практики связаны с обогащением медицинских данных в том числе немедицинской информацией об образе и условиях жизни пациентов.

В тематических исследованиях отмечается, что необратимое обезличивание персональных данных возможно только в течение короткого периода времени и требует регулярной переоценки «сохранения» анонимизированных данных таковыми, что делает анонимизацию столь же ресурсоемким процессом, как и запрос согласия на обработку персональных данных[40].

При этом следует отметить, что в Европе в течение нескольких лет высказывались опасения по поводу «чрезмерной защиты» персональных данных в GDPR[41].

Действительно, когда речь заходит об искусственном интеллекте, необходимо помнить, что доступ к данным является наиболее важной предпосылкой для развития любых инноваций в этой области. В противном случае отсутствие у компаний-разработчиков данных может привести к ситуации, когда огромные ресурсы вкладываются в разработки искусственного интеллекта в области здравоохранения, а успех финансируемых исследований фактически становится недостижимым.

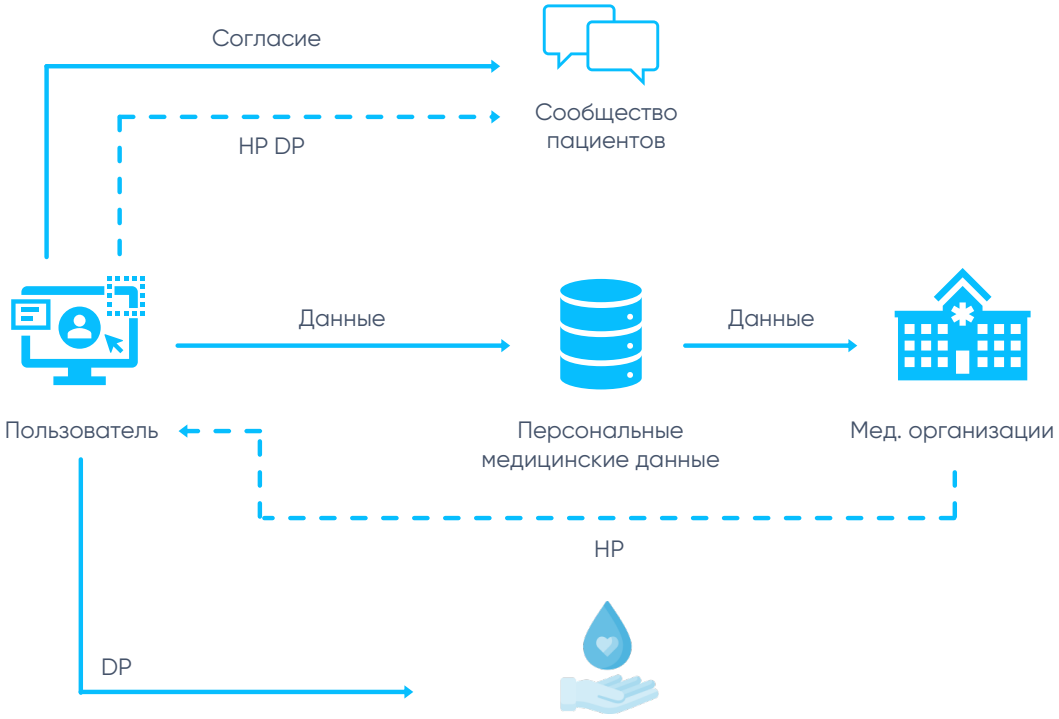
Эффекты от свободного обмена медицинскими данными в защищенном контуре



Какие еще источники данных существуют? Проект Humanscape (Южная Корея)

Humanscape – это блокчейн-платформа для обмена медицинскими данными, которая дает пациентам полный контроль над собственными медицинскими данными (PGHD) и позволяет фармацевтическим компаниям, врачам и медицинским организациям использовать сведения для поиска новых вариантов лечения и оптимизации существующих. С помощью личного профиля здоровья цифровой платформой осуществляется сбор медицинских данных (PGHD). Humanscape систематически организует и сохраняет их в базе данных[42].

Humanscape способствует развитию исследований в области неизлечимых заболеваний и разработки новых лекарств. Применение блокчейн-технологий в процессе управления медицинскими данными пациентов обеспечивает безопасный обмен и хранение такой информации. Все сведения о заболеваниях, регистрируемых пациентами в Humanscape, шифруются и впоследствии могут быть использованы только в четко ограниченных целях. Пациенты также получают компенсацию за публикацию своих данных на платформе[43].



Пользователи делятся на платформе своими медицинскими данными (болезни, симптомы и побочные эффекты, медицинские записи) в обмен на **HP (баллы, которые можно обменять на токены HUM)**, которые выдаются в качестве вознаграждения. Часть вознаграждения выдается в виде **DP (баллы на благотворительность)**, которые можно направить на благотворительность[44].

2. Регуляторные барьеры в России

Регуляторные барьеры в управлении данными в сфере здравоохранения

Медицинские данные пациента содержат сведения, которые позволяют поставить диагноз и назначить лечение. К сожалению, даже опытные врачи не всегда видят полную картину заболевания, потому что данные в медицинской карте не структурированы, а история болезни может быть слишком объемной.

В области здравоохранения большая польза наблюдается от использования больших массивов данных. От того, насколько грамотно налажено управление большими массивами медицинских данных зависит не только эффективность медицинских учреждений, но и здоровье и благополучие людей. Одним из направлений управления данными в медицине является применение технологий на базе искусственного интеллекта (ИИ), где крайне важна автоматизация сбора данных в медицинских учреждениях, чтобы впоследствии на них можно было «обучать» алгоритмы. Ключевым является доступ к данным, а также качество исходных данных для анализа и обучения с целью формирования «валидированных» дата-сетов по самым разным областям медицинских знаний. Чем больше будет данных, пригодных для обучения, тем быстрее удастся «обучить» алгоритмы искусственного интеллекта при принятии решений о диагностике и лечении пациента.

Какие недостатки существуют в текущих реалиях обработки данных в медицинских целях?

Прежде всего, подавляющее большинство медицинских данных являются персональными данными. Это информация о состоянии здоровья человека, результаты клинических исследований, диагнозы, история обращений в медицинские учреждения, данные об образе жизни и привычках, данные, полученные от носимых устройств и мобильных приложений (например, показатели индивидуального здоровья, данные о местоположении, поведенческие характеристики и т. д.), личная информация.

Часть этих данных попадает под категорию конфиденциальных данных, защищенных режимом врачебной тайны. Статья 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» относит к врачебной тайне сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении. Далее в докладе обсуждаются наиболее существенные регуляторные барьеры.

1. Согласие на обработку данных не панацея

Первая проблема заключается в том, что, когда речь идет о защите прав отдельных лиц, субъектов персональных данных, получение согласия на обработку персональных данных не всегда является панацеей. Хотя согласие на обработку персональных данных важно, процедура его сбора может создать ряд проблем как для медицинских организаций, так и для граждан. «Назойливый» сбор согласий на обработку персональных данных может привести к потере заинтересованности или даже ценности в предоставляемых услугах для лица, чье согласие запрашивается.

Яркий пример – неудачная попытка сбора персональных данных после землетрясения и цунами в Японии 11 марта 2011 г. На уровне регионов (префектур, районов и муниципалитетов) действуют свои требования к защите персональных данных субъектов персональных данных. Во многих случаях требования актов местного самоуправления запрещают предоставление персональных данных третьим лицам, за исключением случаев, установленных законом (например, наличие согласия лица на передачу персональных данных третьим лицам, требование закона, заключение специального Совета по защите персональных данных, созданного органом местного самоуправления и др.).

После катастрофы 2011 года (известной в Японии как Великое восточно-японское землетрясение) частные организации в попытке оказать поддержку пострадавшим с ограниченными возможностями запросили персональные данные у региональных органов, большинство из которых отказались предоставлять данные из-за отсутствия согласия субъекта персональных данных на передачу персональных данных третьим лицам. Примерно 60% жертв стихийного бедствия были в возрасте 65 лет и старше, а уровень смертности людей с ограниченными возможностями был в два раза выше, чем здоровых людей.

Таким образом, можно сказать, что сложность сбора согласия на обработку персональных данных ограничила возможность оказания помощи уязвимым слоям населения.

Получается, что архаичность порядка сбора персональных данных может не только повлечь серьезные последствия при оказании медицинской помощи, но и в принципе создать трудности для граждан.

Так, например, эксперты Бенольель и Бехер изучили читабельность 500 самых популярных политик конфиденциальности данных цифровых платформ США, включая Google, Facebook, Uber и Airbnb, и обнаружили, что 498 из них представляли сложность «академического уровня». Возникает резонный вопрос: сколько людей на самом деле читают такие политики конфиденциальности данных (или условия обработки данных)? Во всяком случае, чаще всего такие тексты многословны и трудны для понимания. Существует также связанная с этим проблема «усталости от дачи согласия», вызванной постоянными запросами на предоставление согласия[45]. Кроме того, многие пациенты, например пожилые, пациенты с деменцией и другими заболеваниями, при которых происходит деградация памяти, затрудняются давать согласие на обработку персональных данных.

Помимо архаичности сбора согласия на обработку персональных данных, обеспокоенность вызывает неоднозначность правового регулирования в части сбора согласия на обработку персональных данных.

С одной стороны, согласие является лишь одним из законных оснований обработки данных. Так, согласно действующему российскому законодательству персональные данные можно обрабатывать без согласия субъекта, если такая обработка осуществляется в исследовательских целях, при условии обязательного их обезличивания. Однако, с другой стороны, закон о персональных данных ограничивает доступ даже к таким обезличенным данным, потому что медицинские данные чаще всего собираются только для оказания медицинской помощи[46]. Данный пробел в правовом регулировании вызывает озабоченность, поскольку риск нарушения законодательства о персональных данных не позволяет в полной мере реализовывать потенциал в области медицинских технологий.

Опыт Великобритании

Регуляторные барьеры в области обработки медицинских данных аналогичны тем, что существуют в России. Анонимизация (необратимое обезличивание) персональных данных признается труднодостижимой на практике и может снизить полезность соответствующего набора данных. Простое удаление идентификаторов может привести к получению псевдонимизированных данных, которые считаются персональными данными и составляют объект регулирования законодательства о защите персональных данных (GDPR UK)[47].

Опыт Южной Кореи

Последние поправки в закон Южной Кореи о защите персональных данных (PIPA)[48] позволяют обрабатывать и передавать обезличенные медицинские данные без согласия пациента. Однако на протяжении многих лет осуществить сбор биологических образцов и медицинских данных, необходимых для проведения исследований, было практически невозможно из-за барьеров, заложенных в **законе о биоэтике и безопасности**[49].

2. Ограниченность доступа к медицинским данным

Несмотря на развитие искусственного интеллекта в здравоохранении, доступность данных остается серьезной проблемой в данной сфере. Объем данных растет экспоненциально с каждым днем, а доступ к ним все еще ограничен. К примеру, в 2010 году, по оценкам экспертов, медицинские данные удваивались каждые 3,5 года. В 2020 году медицинские данные удваивались уже каждые 73 дня[50].

Увеличение общего объема медицинских данных подчеркивает необходимость совершенствования механизма обеспечения доступности исследователей, медицинских работников и разработчиков к таким данным. Использование медицинских данных имеет первостепенное значение для развития инноваций и их использования в национальной системе здравоохранения.

Однако доступ к персональным данным о состоянии здоровья, и особенно к данным, защищенным режимом врачебной тайны, строго ограничен. Более того, на практике ученые, исследователи и разработчики не имеют доступа к медицинским данным из ЕГИСЗ для формирования аналитики и развития систем, основанных на ИИ. Для того чтобы у разработчиков была возможность создать полезные для общества системы ИИ, необходимо решить множество правовых вопросов, связанных с доступом к таким данным и порядком их обработки.

В частности, в законодательстве не определены правила и требования доступа к данным в интегрированной электронной медицинской карте и получение оттуда информации в обезличенном виде. Данный пробел в законодательстве тормозит развитие искусственного интеллекта в медицинской отрасли. Смысл защиты персональных медицинских данных – в осторожном регулировании, а не в их недоступности. При этом важно формировать не только правовые, но и этические нормы использования медицинских данных.

Все ресурсы и усилия, которые в настоящее время направлены на разработку ИИ, могут быть потрачены впустую, если проблема доступности к данным не будет должным образом решена.

Опыт Европейского союза

Аналогичная озабоченность среди экспертов присутствует и за рубежом. В этом контексте следует отметить, что проектируемый нормативный правовой акт Европейского союза об искусственном интеллекте (Законопроект об ИИ ЕС)[51], например, устанавливает высокие требования к качеству и количеству данных для обучения, валидации и тестирования, а также к выборке данных для обеспечения необходимой гетерогенности (разнородности) с целью охвата соответствующих групп пациентов (подгрупп) в предполагаемых клинических условиях (статья 10 Законопроекта об ИИ ЕС)[52]. Для реализации проектируемой нормы экспертами отмечается необходимость обеспечения широкого доступа к накапливаемым медицинским данным.

В связи с этим страны Европейского союза ведут работу по разработке регулирования доступа к медицинским данным с целью предоставления разработчикам «топлива» для развития искусственного интеллекта в сфере здравоохранения, учитывая при этом риски защиты персональных данных.

Сбор данных усложняется отсутствием единообразия в подходах ввода и хранения данных основными пользователями медицинских информационных систем (см. раздел 2 предыдущей главы). В медицинских учреждениях могут быть установлены разные информационные системы, которые предусматривают собственные правила ввода и хранения данных. Более того, несмотря на то что **Приказом Минздрава № 947[53] о ведении медицинской документации в форме электронных документов снято существующее ранее требование о дублировании медицинской документации в бумажном виде, существенная часть медицинских записей по-прежнему ведется только в бумажной форме.**

Между двумя крайностями «данные должны быть доступны всем» и «данные не должны быть доступны никому» лежат компромиссные варианты порядка обращения обезличенных данных – через дата-посредников. Поскольку сейчас медицинские данные выделены в специальную категорию особо чувствительных данных и не могут обрабатываться без согласия субъекта даже в обезличенном виде, институт дата-посредников позволит разработчикам получать доступ к дата-сетам в защищенном контуре, а экспериментальный правовой режим даст возможность протестировать правовую гипотезу (подробнее в следующей главе).

Марина Ляшенко
Эксперт по финансовому рынку, Ассоциация Финтех

От первого лица

В цифровом мире бесшовный оборот данных является определяющим фактором для возможности реализации потребностей граждан во всех отраслях. Медицина не является исключением. Новые ритмы жизни не оставляют шанса бумажному документообороту в медицине. Переход на цифровые форматы документов будет способствовать повышению качества медицинских и сопряжённых услуг, в том числе в сфере медицинского страхования. Переход на электронное взаимодействие медицинских и страховых компаний возможен при комплексном подходе, включающем нормативное регулирование и должных уровень цифровизации отраслей.

Подробнее со взглядом российских и международных экспертов в отношении института дата-посредничества можно ознакомиться в подготовленном АНО «Цифровая экономика» аналитическом отчете «Дата-посредники: организации по управлению персональными данными».

3. Необходимость валидации данных

Неменьшую обеспокоенность вызывает вопрос о необходимости валидации собранных медицинских данных для их обработки с использованием систем искусственного интеллекта. Вопросу наличия высококачественных исходных данных для машинного обучения должно быть уделено особое внимание, если рассматривается задача реализации потенциала искусственного интеллекта в сфере здравоохранения. Прежде всего необходимо задать вопрос: нужно ли предоставлять доступ только к валидированным данным высокого качества или достаточно сырых материалов, которые могут быть обработаны искусственным интеллектом?

Электронные медицинские базы данных значительно расширяются как по объему, так и по охвату имеющихся данных. Для разработчиков в области здравоохранения представляется очень привлекательным максимально использовать эти данные[54].

К сожалению, использование регулярно собираемых данных из медицинских карт потенциально приводит к ухудшению качества данных. В частности, такие данные могут не соответствовать действительности или могут быть собраны не в исследовательских целях, а скорее для внутреннего управления или финансового администрирования (поэтому могут не иметь для аналитики никакого значения). Такие данные не всегда пригодны для машинного обучения. Поэтому важно учитывать качество данных, прежде чем они смогут служить источником для аналитики в медицинских целях.

Данные пациентов могут храниться в разных медицинских учреждениях, в каждом из которых используются свои системы и базы данных, разработаны собственные форматы и требования к ведению документации. Часть информации может храниться в бумажном виде. Это затрудняет разработку технологических решений, особенно решений, основанных на системах искусственного интеллекта, поскольку для построения эффективных моделей требуются обширные структурированные дата-сеты.

Поиск качественных медицинских наборов данных – задача тяжелая. Поиском редких данных в различных источниках и организациях призваны заниматься дата-посредники. Качественные наборы данных получаются, когда разработчик или дата-посредник четко знает, какие данные и с какой целью собираются. При этом, если качественно отстраивать процедуры разметки данных, можно повысить и точность решений, построенных на их основе.

Эксперты описывают качественные данные как «данные, которые имеют ценность для аналитики»[55]. В настоящем аналитическом отчете мы используем термин «валидация» для обозначения процесса оценки и улучшения качества данных. Преимущество проведения валидации данных заключается в том, что такой процесс позволяет оценить данные с точки зрения их точности.

Оценка качества (валидация) данных особенно важна в исследованиях, использующих данные из нескольких источников. Сбор из большого количества источников предоставит либо больше случаев «расхождений» из-за наличия некачественных данных (не отражающих реальность), либо дополнительную информацию для получения необходимого результата (исследования, диагноза и т. д.). Необходимость полной валидации и чистки некачественных данных зависит от цели обработки. Для одних бизнес-моделей достаточна приблизительная аналитика, для других, например для аналитики в медицинских целях (постановка диагноза) или определения вероятности дефолта должника, нужны «чистые» данные, чтобы был максимально точный прогноз и минимальное количество ложных показателей. Наличие некачественных данных может быть результатом сбора данных из разных источников с разными системами кодирования, связывания дополнительной информации (например, из внешних источников данных). На каждом этапе привязки несвязанные записи могут привести к выбору неполных и , возможно, не отражающих действительность данных. Однако существующие системы валидации редко учитывают связь с несколькими источниками. Таким образом, то, насколько качественно собираются данные для аналитики, ничуть не менее важно, чем сам процесс валидации.

4. Международный опыт

Технологии искусственного интеллекта в здравоохранении нуждаются в данных о пациентах для разработки модели искусственного интеллекта на этапах обучения, валидации и тестирования. Такие данные о состоянии здоровья часто первоначально

собираются для целей, отличных от разработки технологий искусственного интеллекта. Для вторичного использования таких данных требуется отдельное правовое основание, например согласие пациента.

В Европейском союзе основным источником права в этой области является Общий регламент по защите персональных данных (General Data Protection Regulation, GDPR), который подлежит прямому исполнению во всех государствах – членах ЕС. GDPR преследует две цели:

1. защитить персональные данные, то есть данные, которые можно связать с физическими лицами без особых усилий, и

2. достичь более высокого уровня гармонизации методов защиты данных.

Обработка персональных данных в ЕС требует наличия согласия или иного законного основания (статья 6 GDPR). Согласие субъекта данных определяется как добровольное, конкретное, информированное и однозначное волеизъявление, в котором субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных (пункт 11 статьи 4 GDPR).

Кроме согласия, в GDPR выделяется еще 5 законных оснований для обработки персональных данных (статья 6):

1. обработка необходима для исполнения договора, в котором субъект данных является стороной, или для реализации по поручению субъекта данных шагов, предшествующих заключению договора;

2. обработка необходима для выполнения правового обязательства, возложенного на оператора персональных данных (controller);

3. обработка необходима для защиты жизненно важных интересов субъекта данных или другого лица;

4. обработка необходима для выполнения задачи в публичных интересах или в рамках осуществления государственной власти, доверенной оператору персональных данных;

5. обработка необходима для целей, вытекающих из законных интересов, преследуемых оператором персональных данных или третьим лицом.

К специальным категориям данных GDPR относит, в частности, персональные данные, касающиеся здоровья, и генетические данные. В статье 9 GDPR устанавливается общий запрет на обработку специальных категорий данных, за исключением ряда случаев:

1. когда субъект персональных данных дал явное согласие для одной или нескольких установленных целей;

2. когда обработка необходима по причинам общественного интереса в области общественного здравоохранения;

3. для научных, исторических исследований или статистических целей (статья 9(2) (a), (i) и (j)).

В настоящем разделе рассмотрим вкратце все три основания для обработки медицинских данных.

Согласие. Для получения явного согласия оператор персональных данных должен предпринять дополнительные меры[56]:

- получение письменного согласия субъекта, удостоверенного его подписью;
- в цифровом или онлайн-контексте: заполнение субъектом электронной формы, отправка электронного письма, загрузка отсканированного документа, содержащего подпись субъекта, использование электронной подписи;
- получение согласия в устном виде: если оператор персональных данных сможет доказать, что при регистрации такого заявления были соблюдены все необходимые требования;
- получение согласия по телефону: если информация о выборе является справедливой, понятной и четкой и у субъекта данных запрашивается конкретное действие (например, нажатие кнопки или предоставление устного подтверждения);
- двухфакторная идентификация: например, сочетание электронного письма с сообщением о намерении начать обработку данных, целях обработки и другой необходимой информации, с отправкой ответным письмом явно выраженного подтверждения субъектом (в форме «я согласен») и последующей отправкой субъекту верификационной ссылки, по которой он должен перейти, или смс-сообщения с кодом подтверждения соглашения.

В Преамбуле к GDPR дополнительно указывается, что изъятия из запрета на обработку специальных категорий персональных данных допускаются, если они предусмотрены в праве Европейского союза или национальном праве государства – члена ЕС, если это оправдано с точки зрения общественного интереса. В отношении данных о состоянии здоровья такое изъятие может быть сделано для целей здравоохранения и управления медицинскими услугами[57]. К согласию на обработку специальных категорий данных предъявляются особые требования – одновременно с требованиями добровольности, конкретности, информированности и недвусмысленности, такое согласие должно быть явным.

Получение явного согласия является самым часто используемым основанием для обработки медицинских данных. Европейские эксперты отмечают взаимосвязь института согласия пациента на оказание медицинской помощи и согласия на сбор данных, необходимых для оказания медицинской помощи[58]. Взаимосвязь между данными и оказываемой медицинской помощью показательна, в частности тем, что регуляторы из двенадцати государств – членов Европейского союза предусмотрели согласие (статья 6(1)(a) вместе со статьей 9(2)(a) GDPR) в качестве **одного из оснований для сбора данных пациента и их обработки для оказания ему медицинской помощи**. Такая национальная политика указывает на то, что, хотя согласие является важным аспектом обработки данных в медицинских учреждениях, оно не является единственным. Согласие, как определено в статье 4(11) GDPR, должно быть дано добровольно и в контексте отношений, в которых субъект персональных данных имеет право отказать в даче согласия без какого-либо ущерба для себя.

Согласно Руководящим принципам 05/2020 о согласии в соответствии с Регламентом 2016/679[59] подчеркивается, что «согласие может быть только оценкой соблюдения законодательства государств – членов ЕС в отношении обработки медицинских данных в рамках GDPR, а также соответствующим законным основанием, если

субъекту данных предлагается контроль и реальный выбор в отношении принятия или отклонения предлагаемых условий без ущерба для себя»[60]. Поэтому включение согласия в качестве одного из правовых оснований может быть истолковано несколько иначе. Сбор согласий чаще всего осуществляется для обеспечения гарантии соблюдения законодательства, а не как правовое основание для обработки данных само по себе. Если обработка данных требуется по закону, как это часто бывает в случае сбора данных в медицинских учреждениях, то обычно согласие будет лишь дополнительной гарантией от нарушения действующего законодательства.

Общественный интерес

Обработка данных по причинам, представляющим общественный интерес в области здравоохранения, а также для научных, исторических исследований или статистических целей, относится ко вторичному использованию данных. **Вторичное использование данных** предполагает обработку данных, хранящихся в базах данных первичного использования, таких как системы электронных медицинских карт (EHR), реестры заболеваний, которые собирают данные для расчета уровня заболеваемости и распространенности на национальном или региональном уровне[61].

Примерами обработки данных по причинам, представляющим общественный интерес могут служить: обработка данных в гуманитарных целях, в том числе для контроля эпидемий и их распространения, или в чрезвычайных ситуациях гуманитарного характера, в частности во время техногенных или природных катастроф.

Исследовательские цели

Обработка персональных данных допускается для научных или исторических исследований государственными (университетами, государственными лабораториями и исследовательскими институтами) и частными организациями (третьими сторонами, не являющимися контролером (аналог российского оператора) данных), включая фармацевтические организации, разработчиков, а также страховые организации[62].

Существует два типа обработки (использования) данных, когда речь заходит об «обработке медицинских данных для научных или исторических исследований»[63]:

1. обработка персональных медицинских данных, которая предполагает использование данных, непосредственно собранных в целях научных исследований («первичное использование»)[64];

2. обработка персональных медицинских данных, которая предполагает использование данных, первоначально собранных для другой цели («вторичное использование»)[65].

В соответствии со статьей 6(4) GDPR персональные данные могут быть повторно обработаны для целей, отличных от целей, указанных при сборе персональных данных, только если они **совместимы** с этой целью (принцип «ограничения цели»). Однако, когда речь заходит об обработке данных для исследовательских целей, положения статьи 6(4) GDPR следует рассматривать в сочетании со статьей 5(1)(b) GDPR, которая устанавливает, что повторная обработка данных для научных целей в соответствии со статьей 89(1) GDPR считается совместимой с основной целью.

Следует иметь в виду, что Европейский надзорный орган по защите данных (European Data Protection Supervisor, EDPS) в своих информационных письмах, основываясь на статье 159 GDPR, проводит различие между «подлинными исследованиями» и иными исследованиями (EDPS 2020[66]). По мнению иностранных экспертов,

исследования должны соответствовать методологическим требованиям, стандартам добросовестности исследований (KNAW 2018[67]) и быть направлены на то, чтобы способствовать достижению общественных интересов[68].

В России, также как и во всех развитых странах (страны – члены ЕС, Великобритания, Китай), оператор персональных данных должен обладать законным основанием для сбора и обработки персональных данных. Таким основанием может выступать согласие субъекта либо иные случаи обработки, перечисленные в статье 6 Закона 152-ФЗ. В соответствии с пунктом 9 статьи 6 Федерального закона «О персональных данных» обработка персональных данных без согласия субъекта допускается для статистических или иных исследовательских целей **при условии обезличивания таких данных.**

Однако в экспертном сообществе не утихают споры относительно однозначности термина «исследовательские цели», а также круга субъектов, которые могут осуществлять исследовательскую деятельность (например, только государственные институты или частные научные и исследовательские организации в том числе). Можно ли в таком случае говорить о любом исследовании или исследование должно преследовать достижение общественно значимых целей?

На практике такая неясность в отношении терминов «исследование» и «исследовательские цели» создает затруднения для анализа собранных данных и их передачи для анализа третьим лицам.

GDPR оставляет государствам-членам возможность предусматривать исключение из национального законодательства, когда обработка данных осуществляется в общественных интересах, в статистических, научных или иных исследовательских целях[69]. Так, например, страна – член ЕС вправе самостоятельно определять методы псевдонимизации (необратимо обезличенные данные), дополнительные ограничения на обработку персональных данных в исследовательских целях[70]. В дополнение к GDPR71, национальное законодательство в сфере здравоохранения и биобанкинга[72] также может включать специальные условия доступа к медицинским данным[73]. Поэтому страны ЕС по-разному регулируют обработку медицинских данных. В этом отношении более консервативная Германия и более либеральная Финляндия являются примерами стран, которые кардинально отличаются своими подходами к управлению данными в сфере здравоохранения.

Как Европейское пространство данных о здоровье защищает конфиденциальность граждан?

Не подлежащие идентификации данные

У исследователей и профильных организаций есть доступ к данным, но не к личности стоящего за ними человека

Анонимность и высокие стандарты кибербезопасности

Работа с данными возможна в рамках защитных «пузырей», данным присвоены псевдонимы

Ограничения доступа

Доступ к базам данных имеют только разработчики, исследователи, медицинские организации и только по причинам, представляющим общественный интерес

Финляндия

Финский подход к обороту медицинских данных отражен в законе о повторной обработке медицинских и социальных данных[74], который регулирует порядок доступа к данным пациентов и обмена ими, а также выдачи разрешений на использование этих данных специальным органом (Health and Social Data Permit Authority) – Findata. Findata – это агентство по управлению информацией в социальном секторе и здравоохранении. Оно дает рекомендации по использованию данных в науке и следит за обеспечением их эффективной защиты. Оно выдает разрешения, в частности, на использование медицинских данных для научных исследований, в преподавательской сфере, для разработки инноваций, формирования стратегий в интересах общества.

Следует отметить, что Финляндия стала примером политики, ориентированной на открытый обмен данными и преобразующей регулирование для развития искусственного интеллекта[75]. В Финляндии согласие на обработку персональных данных не требуется при сборе персональных данных в национальные реестры здравоохранения. Однако доступ к собранным данным подробно регулируется нормативными правовыми актами и регламентами об информационной безопасности[76]. Более того, закон о биобанках 2012 года[77], над которым в настоящее время ведется работа по доработке, позволяет использовать биологические образцы биобанка (крови, плазмы, ДНК, РНК, тканевых материалов и т. д.), а также связанные с ними данные в исследовательских целях без получения (повторного) согласия для каждого исследовательского проекта (образцы биобанка могут также быть связаны с данными о состоянии здоровья из национальных реестров). Финляндия входит в число стран ЕС с самыми развитыми цифровыми экономиками и предоставляет онлайн-сервис, который граждане используют для просмотра информации о своем здоровье из разных источников[78].

Также следует отметить, что обработка данных для исследовательских и статистических целей осуществляется без повторного сбора согласия на обработку персональных данных субъекта персональных данных. Однако орган, выдающий разрешения на передачу данных, (Findata) устанавливает минимальный объем данных, необходимый для обработки в каждом конкретном случае[79].

Германия

Финский подход отличается от немецкого, который ориентирован на полный контроль над данными и , при котором обработка медицинских данных обычно проводится с согласия пациента. Например, согласие субъекта персональных данных является правовым основанием для обработки любых данных, хранящихся в недавно запущенной электронной карте пациента (elektronische Patientenakte или ePA). Обработка данных для научных исследований в общественных интересах может осуществляться без согласия субъекта персональных данных, если соблюдаются требования, установленные в Федеральном законе о защите персональных данных[80].

Новый закон (DVG) предусматривает также введение ряда цифровых инноваций в процесс медобслуживания. В их числе, например, подключение к инфраструктуре телемедицины и выдача электронных рецептов (eRezept или ePrescription). Последняя инновация внедряется даже в рамках общеевропейского проекта, то есть как карточки, так и выписанные рецепты будут действовать в рамках всего Евросоюза. Представлены система электронной документации об услугах по уходу и лечению, цифровое управление выдачей лекарств, меры ИТ-безопасности и межотраслевые телемедицинские сетевые структуры.

1. Регулирование медицинских данных

С точки зрения законодательства персональные медицинские данные относятся к специальной категории персональных данных, которая регулируется следующими нормативными правовыми актами:

- Закон о защите персональных данных (разделы 22 и 27); Закон о защите от инфекционных заболеваний (раздел 9 и далее); Закон о лекарственных препаратах (раздел 40); Закон о медицинских изделиях (раздел 20); Кодекс социального обеспечения и др.

- Закон о цифровом здравоохранении, Постановление о приложениях для цифрового здравоохранения и Закон о защите данных пациентов.

2. Анонимизация персональных медицинских данных

- В некоторых случаях немецкий закон о защите данных требует, чтобы обрабатываемые медицинские данные были обезличены. Например, данные о состоянии здоровья, обрабатываемые в научных, исследовательских или в статистических целях, должны пройти процедуру анонимизации (раздел 27 (3) закона о защите данных).

- Специальные требования к анонимизации предусмотрены в Руководстве о медицинских данных, опубликованном Министерством экономики Германии.

3. Информационная безопасность

Приложения в сфере цифрового здравоохранения должны соответствовать требованиям безопасности персональных данных в соответствии с современным уровнем техники, учитывая вид обрабатываемых данных.

Предполагается, что пациент сможет получать доступ к своим личным данным через приложение. Сначала пациент вводит свой PIN-код, а затем в качестве подтверждения TAN – одноразовый код, присланный в смс-сообщении. Такая двухуровневая система безопасности облегчит пациентам доступ к своим персональным данным, при этом сохранив уровень информационной безопасности. Передача информации таким способом должна осуществляться лишь с согласия самого пациента. То есть «мобильную больничную карту» пациент оформляет только по своему желанию.

«Умные» медицинские помощники уже разрабатываются крупными компаниями, и активнее всех это делают компании из Великобритании, США и Израиля. Ниже мы рассмотрим опыт регулирования обработки медицинских данных в этих странах.

Великобритания

1. Регулирование медицинских данных

Обработка медицинских данных регулируется в основном GDPR Великобритании, законом о защите данных (Data Protection Act, DPA) и законами о конфиденциальности данных, которые приняты в разных частях Великобритании (Англия, Северная Ирландия, Шотландия и Уэльс)[81].

GDPR Великобритании[82] устанавливает ограничения на обработку медицинских данных, обязывая операторов предварительно уведомлять об обработке данных. Для обработки медицинских данных операторам требуется явное согласие отдельных лиц. Оно должно быть конкретным, обоснованным и добровольным.

Закон о защите данных также содержит нормы, регулирующие использование автоматизированных средств для принятия решений, которые имеют юридические или «по существу аналогичные» последствия для отдельных лиц[83]. Например, законом о защите данных регулируются вопросы обработки данных с помощью программного обеспечения (например, искусственного интеллекта), в том числе когда такие автоматизированные системы не просто помогают при принятии решений, но и заменяют весь процесс постановки диагноза в медицинских учреждениях[84].

GDPR Великобритании[85] и DPA[86], как правило, запрещают использование персональных медицинских данных без согласия субъекта персональных данных, но предусматривают исключения: например, разрешена обработка персональных данных для оказания медицинской помощи, а также в исследовательских и иных научных целях и в общественных интересах. Обработка в исследовательских целях без согласия субъекта персональных данных допускается при условии, что такие исследования не влекут за собой принятие решений, затрагивающих субъект персональных данных, если только исследовательский проект не одобрен специальным комитетом по этике.

В настоящий момент правительство Великобритании ведет работу по внесению изменений в закон о защите данных[87], что может также привести к изменениям в GDPR Великобритании. Основой таких изменений является доклад британских экспертов о необходимости создания безопасной среды для обмена большими массивами медицинских данных «Данные спасают жизни: изменение системы здравоохранения и социального обеспечения с помощью данных». Доклад-стратегия опубликован в начале 2022 году Департаментом здравоохранения и социального обеспечения Великобритании (DHSC). Авторы доклада предлагают способы упрощения порядка отказа от обмена данными и улучшения доступа к записям врачей общей практики в приложении NHS, которое планируется реализовать к ноябрю 2022 года[88].

Представляя стратегию на саммите HealthTech на Лондонской технологической неделе, министр здравоохранения Саджид Джавид объявил о создании надежной исследовательской среды (TREs) – защищенной среды обмена данными – для того, «чтобы исследователи и разработчики могли получить безопасный доступ к связанным данным NHS с высочайший уровнем конфиденциальности»[89].

2. Анонимизация персональных медицинских данных

Британский Совет по медицинским исследованиям (MRC) опубликовал руководство по идентификации, анонимизации и псевдонимизации персональных данных в рамках исследовательской деятельности. Руководство напоминает исследовательским организациям, что Общий регламент по защите персональных данных (GDPR) применяется к медицинским данным, обрабатываемым в исследовательских и иных научных целях, и содержит ряд рекомендаций, которые должны иметь в виду участники исследования. Руководство было разработано при участии Управления комиссара Соединенного Королевства по информации (ICO).

- Данные о состоянии здоровья, обрабатываемые в научных, исследовательских или в статистических целях, должны пройти процедуру анонимизации[90].
- Специальные требования к анонимизации предусмотрены в Руководстве об обезличивании медицинских данных[91].

США

Основным источником регулирования медицинских данных в США является Закон о преемственности и подотчетности медицинского страхования США 1996 г. (HIPAA)[92].

Сфера применения HIPAA[93] охватывает лишь небольшую часть отрасли здравоохранения – закон стал главным документом, закрепляющим право пациентов на доступ к своим персональным медицинским данным и обязанность организаций защищать их персональные медицинские данные. Несмотря на то что HIPAA устанавливает ограничения на использование персональных медицинских данных, он был принят в первую очередь для обеспечения обмена данными о пациентах, закрепляя правовые рамки для законной и безопасной передачи данных. Правила защиты персональных медицинских данных, установленные HIPAA, не распространяются ни на обезличенные данные, ни на какие-либо другие данные, помимо PHI. Данный закон распространяется на следующие организации: **поставщики медицинских услуг, страховые медицинские организации, операторы по сбору данных, контрагенты (аналитики).**

Второй источник правового регулирования медицинских данных в США – это Закон о применении медицинских информационных технологий в экономической деятельности и клинической практике (HITECH[94]), который дополнил HIPAA в 2009 году. HITECH регулирует обработку и порядок раскрытия «охраняемой законом информации о состоянии здоровья» – персональных медицинских данных (PHI).

HITECH усилил ответственность за несоблюдение норм о защите персональных медицинских данных и требований к обработке данных. Основной целью HITECH было ускорение внедрения электронных медицинских карт (EHRs) и новых технологий в сфере здравоохранения, которые призваны улучшить качество оказания медицинской помощи. Ужесточение требований к защите персональных медицинских данных в HIPAA – это способ снизить риски, связанные с накоплением больших массивов медицинских данных в единой информационной системе здравоохранения[95].

Закон о запрете дискриминации на основе генетической информации (Genetic Information Nondiscrimination Act, GINA[96]) вступил в силу в 2008 году, когда на американский рынок поступили недорогие клинические диагностические генетические тесты, доступные потребителю. GINA запрещает работодателям требовать или финансово стимулировать сотрудников раскрывать свои генетические данные, персональные медицинские данные или истории болезни семьи; а также дискриминировать лицо при приеме на работу на основе генетических данных или истории болезни.

Штаты вправе принимать локальные нормативные правовые акты, устанавливающие требования к обработке персональных медицинских данных, внося свой вклад в «лоскутное одеяло» законов о защите персональных данных в США.

Все 50 штатов и федеральный округ Колумбия приняли законы, закрепляющие обязанность организаций уведомлять о случаях нарушения правил по обеспечению безопасности персональных данных при их обработке. Из них 16 штатов предусмотрели специальные правила уведомления о нарушениях правил обработки медицинских данных или истории болезни, еще 7 штатов включили в данный перечень биометрические данные и медицинские данные, касающиеся страхования[97].

Израиль

Израиль начал оцифровку медицинских данных 20 лет назад, намного опередив многие другие страны. В Израиле существует медицинская информационная система, которая включает в себя данные почти 9 миллионов человек.

В апреле 2017 года Минздрав Израиля опубликовал «Стратегию цифрового здравоохранения», в которой изложены ключевые НПА для создания правовой основы цифрового здравоохранения:

- регулирование использования данных о состоянии здоровья (цели, способ использования, пользователи, прозрачность);
- правила использования дистанционной медицинской помощи (порядок предоставления услуги и обязательства поставщика услуг);
- регулирование доступа пациентов к личным электронным медицинским картам,
- положение об определении минимального содержания электронных медицинских карт;
- регулирование порядка обработки ;
- регулирование процессов разработки и обслуживания клинических информационных систем;
- регулирование вопросов кибербезопасности.

1. Регулирование медицинских данных

Основные направления законодательных инициатив включают:

- содействие нормативному регулированию повторного использования медицинских данных;
- поддержка других необходимых направлений регулирования (облако, цифровая подпись);
- поддержка медицинских организаций в обновлении медицинских информационных систем.

2. Обезличивание медицинских данных

Минздрав Израиля выпустил три Информационных письма[98], которые разъясняют правила защиты персональных медицинских данных. Если иное не предусмотрено законом, персональные данные, подлежащие повторному использованию, должны быть обезличены.

3. Информационная безопасность

В июле 2019 года Министерство здравоохранения впервые разрешило медицинским организациям использовать облачные сервисы для хранения персональных медицинских данных.

Сравнительно-правовой анализ

Направление инновационного развития	Страна заимствования	Регулирование в России
Регулирование медицинских данных	Германия, Финляндия, Израиль, Великобритания	С точки зрения законодательства персональные медицинские данные относятся к специальной категории персональных данных. По общему правилу, обработка таких персональных данных не допускается (пункт 1 статьи 10 Закона № 152-ФЗ), за исключением определенных случаев. К таким случаям относятся: обработка в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг (подпункт 4 пункта 1 статьи 10 Закона № 152-ФЗ).
«Регуляторные песочницы»	Израиль, Германия, Сингапур, Южная Корея, Малайзия	31 июля 2020 г. был принят Федеральный закон № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», на базе которого с 2021 года в России возможно будет создание «регуляторных песочниц» в различных областях.
Кибербезопасность	Германия, Финляндия, Израиль, Великобритания	Законодательство Российской Федерации уже предусматривает общие требования к информационной безопасности инновационных продуктов, однако, с учетом развития технологий ИИ и робототехники эти требования в ряде случаев должны быть уточнены.
Единая база данных	Германия, Финляндия, Израиль	Вступило в силу Положение о единой государственной информационной системе в сфере здравоохранения.

III. Преодоление правовых барьеров в области обработки данных в медицине: «лечение» коллизий в законодательстве

1. Обработка данных с использованием систем ИИ в медицине: согласию быть?

Разработчики нейросетевых алгоритмов в области медицины достигли больших успехов в последние несколько лет, однако у таких алгоритмов есть один общий недостаток – они требуют больших массивов данных, доступ к которым в некоторых странах может быть законодательно ограничен.

В частности, эффективность от реализации алгоритмов в области медицины зависит от наличия доступа к медицинским данным. Так, сегодня отсутствуют правила доступа к сведениям, которые собираются в интегрированной электронной медицинской системе (ЕГИСЗ). Без такого «топлива», как данные, медицинский искусственный интеллект не сможет развиваться и приносить пользу врачам и обществу.

Новое немецкое регулирование

1. Врачам разрешено назначать и выдавать пациентам персональные медицинские устройства
2. Расширен доступ разработчиков к данным пациентов для проведения исследований
3. Все застрахованные пациенты вправе потребовать доступ к электронной медицинской карте
4. Взаимодействие пациента и поставщика медицинских услуг, включая выдачу рецептов, полностью переведено на ЭДО
5. Аптеки, медицинские учреждения и больницы обязаны подключаться к защищенным сетям связи

Также необходимо решить проблему правовой неопределенности в отношении обработки таких данных. Обеспокоенность вызывает, например, существующая правовая коллизия в отношении медицинских данных, обрабатываемых системой ИИ. Так, согласно действующему законодательству персональные данные можно обрабатывать без согласия субъекта, если такая обработка осуществляется в исследовательских целях, при условии обязательного их обезличивания. Однако закон о персональных данных ограничивает доступ даже к таким обезличенным данным, потому что медицинские данные чаще всего собираются только для оказания медицинской помощи.

При этом в силу действующего законодательства, а именно Федерального закона «О персональных данных», обработка даже обезличенных данных о состоянии здоровья требует получения согласия субъекта персональных данных в письменной форме. Такое требование обусловлено определением в указанном законе понятия «обезличивание персональных данных», т. е. «действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных». Как видно, обезличенные данные все равно остаются персональными, в силу чего к ним

применяются аналогичные (что и к персональным) требования, в том числе требование о получении письменного согласия (статья 10 Федерального закона «О персональных данных»).

В литературе неоднократно отмечается, что существующие методики обезличивания не позволяют безвозвратно обезличить персональные данные. В связи с этим существует возможность идентификации человека по набору обезличенных данных, особенно в случае объединения информации из нескольких источников. Однако

Французское регулирование оборота медицинских данных

1. Создана государственная система больших данных в области здравоохранения (SNDS), которая дает возможность разработчикам получить доступ к медицинским данным, собранным из больниц, страховых и общественных организаций.

2. Разработчикам и исследователям необходимо пройти ряд процедур и предварительных проверок для получения доступа к обезличенным медицинским данным.

3. В 2019 году во исполнение закона об организации и трансформации национальной системы здравоохранения Франции создана платформа данных Health Data Hub для развития исследований и разработок отдельных проектов.

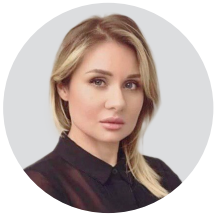
примечательно, что эксперты из MIT в своем исследовании 2022 года количественно оценили потенциальный риск такого рода деобезличивания пациентов и обнаружили, что в настоящее время такой риск деобезличивания чрезвычайно низок, например по сравнению с риском утечки персональных данных.

Большие базы медицинских данных, созданные больницами и другими учреждениями, содержат огромное количество информации о таких заболеваниях, как порок сердца, рак, дегенерация желтого пятна и COVID-19, которая необходима разработчикам и исследователям для поиска их эффективного лечения.

Подробнее со взглядом российских и международных экспертов на эту проблему можно ознакомиться в опубликованном АНО «Цифровая экономика» в феврале 2022 года отчете на тему «Изменение подходов к обороту персональных данных».

Таким образом, регуляторный барьер, который предлагается нивелировать, заключается в необходимости получения письменных согласий на обработку персональных данных пациентов, даже если такие данные будут обезличены (пункт 1 части 1 статьи 6 и пункт 1 части 2 статьи 10 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ).

Снятие регуляторного барьера путем запуска «цифровых песочниц» и последующее масштабирование на общее регулирование отрасли позволят разработчикам обрабатывать обезличенные данные, в том числе обезличенные данные о состоянии здоровья, без получения согласия субъектов персональных данных.



Ольга Гребнева
Руководитель направления, Лаборатория финтех и инноваций САО «ВСК»

От первого лица

Защита интересов граждан должна быть ключевой при решении вопроса доступа к медицинским данным. При этом важно помнить, что излишние требования к обороту медицинских данных и отсутствие сквозных понятий в законодательных актах, в том числе: Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ и Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 № 323-ФЗ создаёт барьеры для получения гражданами бесшовных цифровых сервисов. Возможность управления согласиями и определение именно гражданином какие данные подлежат передаче 3-м лицам позволяют реализовать безопасные сервисы для граждан и повысить скорость и качество оказания медицинских и сопряжённых услуг, в том числе в сфере медицинского страхования.

Опыт Германии

GDPR устанавливает различные требования к данным о состоянии здоровья в зависимости от организации, отправляющей и получающей данные.

Обмен данными между медицинскими работниками в целях диагностики или лечения обычно подпадает под исключение, предусмотренное в статье 9(2)(h) GDPR. Аналогичным образом специалисты могут делиться информацией со страховыми (медицинскими) организациями для выставления счетов на оплату медицинских услуг. Однако следует отметить, что такие данные, согласно GDPR, могут подпадать под режим врачебной тайны.

Обмен между исследовательскими организациями и медицинскими учреждениями предусмотрен статьей 9(2)(j) GDPR и разделом 27 Закона Германии о защите данных (BDSG), согласно которым допускается передача данных без согласия субъекта в научных и исторических целях.

Персональные медицинские данные относятся к специальной категории данных, и к их обработке предъявляются более строгие требования. Раскрытие медицинских данных в общем случае допускается с согласия субъекта, а также в целях оказания медицинской помощи при наличии угрозы жизни и здоровью субъекта, в целях анализа и мониторинга работы системы здравоохранения, по причинам, представляющим общественный интерес в области здравоохранения, в целях проведения исследований в сфере медицины.

В качестве примера можно привести порядок предоставления доступа к данным регистра раковых заболеваний, установленный Законом Германии о трансплантации[99]. Согласно разделу 15g Закона о трансплантации доступ к данным из регистра может быть предоставлен даже без согласия субъекта данных, если получение такого согласия связано с непропорциональными усилиями, а публичный интерес и цель исследования имеют большую ценность для общества. На практике использование дата-посредников (Vertrauensstelle) обеспечивает достаточный уровень защиты данных за счет их обезличивания по умолчанию[100].

Новое немецкое регулирование (Digitales Versorgungsgesetz, DVG[101])

1. С 2020 года врачи вправе рекомендовать пациентам использовать персональные медицинские приложения (digitale Gesundheitsanwendung, DiGA), прошедшие проверку информационной и технологической безопасности Федерального института по лекарственным препаратам и медицинской продукции (Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM).

2. Немецкие государственные медицинские страховые компании обязаны направлять обезличенные демографические данные пациентов (например, уровни доходов, семейное положение, этническое происхождение, пол, гендерная идентичность, возраст) и данные о состоянии здоровья в единую государственную информационную систему. Исследовательские организации и университеты вправе запрашивать доступ к таким данным в исследовательских целях.

3. Все застрахованные пациенты вправе потребовать доступ к своей электронной медицинской карте.

4. Взаимодействие пациента и поставщика медицинских услуг, включая выдачу рецептов, полностью переведено на электронный документооборот (ЭДО).

5. Аптеки, медицинские учреждения и больницы обязаны подключаться к защищенным сетям передачи данных. Все аптеки и больницы/поставщики медицинских услуг обязаны подключиться к немецкой безопасной сети передачи медицинских данных – Gematik.

Опыт Франции

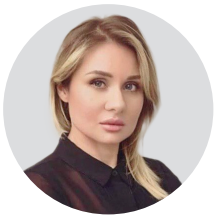
Очевидно, что большое число административных документов содержит персональные данные. В некоторых случаях их обработка подпадает под режим охраняемой законом тайны – врачебной тайны. Врачебная тайна известна законодательству всех развитых стран (например, во Франции, Германии, России). Такой режим требует от оператора персональных данных получения согласия пациента на передачу своих медицинских данных любой стороне, не входящей в состав «медицинской команды». Согласно статье L. 1110-12 Медицинского кодекса Франции[102] медицинская команда – «это группа специалистов, которые непосредственно оказывают медицинскую помощь одному и тому же пациенту, включая проведение диагностического, терапевтического, восстанавливающего инвалидность, анестезиологического или профилактического мероприятия».

Следует отметить, что законодательство предусматривает исключения из общего правила обязательного получения согласия на передачу медицинских данных, например запрет на продажу персональных медицинских данных (статья L. 1111-8, VII Медицинского кодекса Франции[103]) или запрет на использование информации медицинских работников, полученной из рецептов на лекарственные препараты (статья L. 4113-7 Медицинского кодекса Франции[104]).

В 2019 году во исполнение закона об организации и трансформации национальной системы здравоохранения Франции создана платформа данных Health Data Hub

для развития исследований и разработок отдельных проектов. Платформа дает разработчикам и исследователям доступ к большому объему медицинских данных, полученных из различных информационных систем. Платформа собирает данные о состоянии здоровья, формирует дата-сеты и предоставляет разработчикам доступ к ним. Такой подход способствует свободному обмену обезличенными данными с соблюдением необходимых требований законодательства и прав граждан (статья L. 1462-1 Медицинского кодекса Франции[105]).

От первого лица



Ольга Гребнева
Руководитель направления, Лаборатория финтех и инноваций САО «ВСК»

Отнесение обезличенных персональных данных к персональным изменяет их сущность создает нормативные барьеры для обработки. Риски «деобезличивания» возможно снять регламентацией правил и стандартов процесса обезличивания. Разделение понятий даст импульс для развития искусственного интеллекта.

Таким образом, для того чтобы максимально эффективно использовать медицинские данные для развития решений на основе ИИ, предлагается:

- уточнение существующих правовых оснований обработки персональных данных, в том числе уточнение понятия «обработка в статистических и иных исследовательских целях»;
- в рамках экспериментального правового режима нивелировать положение о необходимости получения письменных согласий на обработку персональных данных пациентов, даже если такие данные будут обезличены (пункт 1 части 1 статьи 6 и пункт 1 части 2 статьи 10 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ);
- установление в Федеральном законе «О персональных данных» от 27.07.2006 № 152-ФЗ возможности предоставления согласия на обработку персональных данных в письменной форме «...одновременно на несколько целей, а также нескольким лицам, осуществляющим обработку персональных данных по поручению оператора персональных данных»;
- установление в Федеральном законе «О персональных данных» от 27.07.2006 № 152-ФЗ возможности использования оператором персональных данных ранее собранных данных для иных целей при наличии согласия субъекта персональных данных или иных законных оснований для обработки.

2. Качественные методы обезличивания персональных данных: количество переходящее в качество?

Медицинские данные хоть и являются отдельной категорией, но как по сути своей, так и по законодательству являются специальной категорией персональных данных. Трендом текущего периода является создание таких «качественных» методов обезличивания персональных данных, которые, с одной стороны, не позволяют восстановить персональные данные, с другой стороны, позволяют работать с ними разработчикам искусственного интеллекта. Государство сейчас активно строит соответствующую инфраструктуру для разработчиков, и медицинские данные могут быть ее частью.

Напомним также, что Роскомнадзором, как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации, установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, которые утверждены приказом Роскомнадзора от 5 сентября 2013 года № 996.

Данные методические рекомендации содержат методологию обезличивания персональных данных в информационных системах, а также построение процессов дальнейшей обработки данных, полученных в результате обезличивания. Методические рекомендации содержат анализ процессов автоматизированной обработки обезличенных данных, требований к обезличенным данным и методов обезличивания, позволяющий выделить основные свойства обезличенных данных и методов обезличивания и оценить возможности их применения при решении задач обработки персональных данных с учетом вида деятельности оператора персональных данных и необходимых действий с персональными данными.

В этой связи сегодня особенно важно создать платформу, в рамках которой можно будет проверять качество обезличивания данных, высчитывая уровень или класс обезличенности, отталкиваясь от тех данных в базе, которые на данный момент есть. Как было указано в разделе 1 настоящей главы, пока законодательство четко не разграничивает обезличенные и персональные данные, поэтому вместе с введением института дата-посредничества предлагается разрабатывать методики качественного обезличивания персональных данных.

Основной функцией такого нового субъекта рынка данных, как дата-посредники, является управление данными, включая их сбор, обработку, обезличивание и обмен. В связи с этим возникает большое количество вопросов относительно того, как права граждан и компаний будут защищаться при оказании им услуг по управлению данными. Какие при этом требования законодательства о персональных данных и информации применимы? Какие принципы функционирования дата-посредников необходимо ввести? Достаточно ли действующего законодательства о персональных данных?

Существующие в профессиональной литературе подходы к регулированию дата-посредников, как правило, основаны на разрозненных мерах, а единая концепция защиты прав и интересов граждан и компаний отсутствует. В связи с этим особенно важно сформировать модель регулирования (законодательно закрепив или сформировав кодекс этики), которая отражала бы «надежность» управления данными с помощью дата-посредников. Такой подход должен отражать оптимальную модель дата-посредников, которая максимально возможным способом минимизирует риски, связанные с незаконным обменом данными.

Для этих целей следует определить основные требования к дата-посредникам в части обеспечения информационной безопасности, модели управления данными, порядка обезличивания и сертификации дата-посредников. Предлагаемые опции регулирования следует рассматривать в комплексе с существующим регулированием персональных данных и информации. Также предлагается запустить механизм «регуляторных песочниц», который позволит апробировать и внедрить различные формы дата-посредников.

Подробнее об институте дата-посредников можно ознакомиться в опубликованном АНО «Цифровая экономика» в 2022 году отчете на тему «Дата-посредники: организации по управлению персональными данными».

Таким образом, для обеспечения доступа к качественным наборам данных в целях разработки решений на основе ИИ в области медицины, предлагается:

- Введение института дата-посредничества для организации обмена и управления данными. В число функций дата-посредников входит обезличивание данных, формирование наборов данных на основе запросов разработчиков и предоставление к ним доступа при соблюдении требований, установленных законом и /или договором. На пути регулирования дата-посредников существует несколько принципиальных развилок, и найти верное решение представляется возможным после практической апробации правового механизма путем запуска экспериментального правового режима и в случае успеха масштабирования уже в рамках общего регулирования.

- Уточнение полномочий Роскомнадзора по утверждению требований и методов обезличивания персональных данных.

3. Валидация больших массивов данных: можно ли использовать все данные или необходим их обязательный отбор?

Неменьшую обеспокоенность вызывает вопрос о необходимости валидации собранных медицинских данных для их обработки с использованием систем искусственного интеллекта. Вопросу наличия высококачественных исходных данных для машинного обучения должно быть уделено значительное внимание, если рассматривается задача реализации потенциала ИИ в сфере здравоохранения.

Представляется возможным поддерживать доступ к исследовательским базам валидированных и невалидированных данных для развития систем ИИ в здравоохранении. При этом следует определить, в каких случаях такая валидация данных необходима.

В соответствии с международным стандартом ISO 9000:20153[106] качество наборов данных – это соответствие наборов данных определенным критериям (данные характеристики определяются в каждом конкретном случае). Согласно данному документу обеспечение качества (или так называемая валидация) данных – это процесс профилирования данных для обнаружения несоответствий, неточностей, неполноты и других аномалий в данных, а также выполнение действий по их очистке и агрегированию для того, чтобы улучшить качество больших массивов данных.

В тематических исследованиях чаще всего отмечаются следующие характеристики качественных наборов данных[107]:

1 Точность данных – степень близости результатов наблюдений к истинным значениям или значениям, принятым как истинные. Этот показатель качества обычно используется для измерения качества собранных данных путем сравнения данных из нескольких источников. Точность данных может быть оценена в двух аспектах:

   - точность атрибутов данных – точность наборов значений данных;

- точность моделирования – отсутствие операционных ошибок при сборе данных.

2 Актуальность данных: Дэвид Лошин в своем тематическом исследовании отмечает, что актуальность данных определяет степень соответствия данных моделируемой области на определенный момент времени[108].

3 Достоверность данных отражает показатель качества данных, определяющий насколько корректно данные описывают моделируемую область.

4 Полнота наборов данных – это показатель качества данных, определяющий достаточность заполнения наборов данных и их атрибутов.

Опыт Германии[109]

Раздел 27 (1) Закона BDSG[110]: В отступление от статьи 9 (1) Регламента (ЕС) 2016/679 обработка особых категорий персональных данных, указанных в статье 9 (1) Регламента (ЕС) 2016/679, разрешается также без согласия в целях научных или исторических исследований или в статистических целях, если такая обработка необходима для этих целей и интересы контролера при обработке существенно перевешивают интересы субъекта данных при отказе от обработки данных. Контролер должен принять надлежащие и конкретные меры для защиты интересов субъекта данных в соответствии со вторым предложением раздела 22 (2).

§ 22 II BDSG[111]: В случаях, предусмотренных подразделом 1 (разрешение на обработку особых категорий персональных данных), оператором персональных данных должны быть приняты надлежащие меры для защиты интересов субъекта данных. Принимая во внимание уровень оборудования, затраты на внедрение, характер, объем и цели обработки персональных данных, а также риски различной вероятности нарушения прав и свобод физических лиц, связанных с обработкой персональных данных, такие меры включают, в частности, следующее:

1. технические и организационные меры для гарантирования соответствия обработки персональных данных требованиям, установленным GDPR;

2. меры по обеспечению фиксации случаев введения, изменения или удаления персональных данных;

3. повышение осведомленности работников организации в области персональных данных (под повышением осведомленности работников организации понимается целенаправленное, систематическое повышение уровня знаний работников и формирование необходимых навыков в области информационной безопасности);

4. назначение лица, ответственного за обработку персональных данных (data protection officer);

5. ограничения на доступ к персональным данным контролера и оператора персональных данных;

6. псевдонимизация персональных данных;

7. шифрование персональных данных;

8. меры по обеспечению конфиденциальности, целостности, доступности и устойчивости систем обработки и сервисов, связанных с обработкой персональных данных, включая возможность быстрого восстановления доступа к данным в случае неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов персональных данных (инцидента);

9. регулярное тестирование и оценка эффективности технических и организационных мер по обеспечению безопасности обработки персональных данных;

10. установление локальных правил обработки для обеспечения соблюдения национального законодательства и GDPR в случае передачи или обработки для других целей;

11. оценка соответствия национального регулирования медицинских данных государств – членов ЕС правилам, установленным GDPR.

В России для безопасного и качественного процесса проверки данных различных типов по критериям корректности и полезности для применения в медицинских целях предлагается введение мер, способствующих восстановлению и усовершенствованию процедур контроля и методов валидации, предназначенных для обеспечения целостности обрабатываемых данных.

Резюме международного опыта

	Израиль	США	Великобритания	Южная Корея	Европейский союз		
					Германия	Франция	Финляндия
Основные нормативные акты	Закон о защите данных, 2017; Информационные письма Минздрава.	HIPAA; HITECH; GINA; отдельные законы штатов.	GDPR UK; Data Protection Act, DPA.	PIPA.	**ЕС:** GDPR.		
					BDSG.	Code de la santé publique (Медицинский кодекс Франции).	Secondary Use Act, 2019; Finnish Data Protection Act; Finnish Biobank Act.
Медданные	**Специальная категория персональных данных (предусмотрены специальные требования к обработке медданных)**						
Согласие на сбор и обработку медданных	Если согласие пациента на обработку персональных данных отсутствует, то повторное использование данных разрешено только в случае анонимизации данных (необратимо обезличенных).	При сборе и обработке ПД в исследовательских целях необходимо получить информированное согласие пациента (Федеральные правила проведения исследований); HIPAA устанавливает обязанность медорганизаций получать письменное разрешение для обработки и раскрытия персональных медданных в исследовательских целях.	Оператор обязан предварительно уведомлять пациента об обработке его медданных.	Последние поправки в закон о защите ПД (PIPA) позволяют обрабатывать и передавать обезличенные медданные без согласия пациента.	**ЕС:** В ст. 9 GDPR устанавливается общий запрет на обработку специальных категорий данных за исключением ряда случаев: 1) когда субъект персональных данных дал явное согласие для одной или нескольких установленных целей; 2) когда обработка необходима по причинам общественного интереса в области общественного здравоохранения; 3) для научных, исторических исследований или статистических целей (ст. 9 (2) (a), (i) и (j)). Особенности отдельных стран:		
					Обработка данных для научных исследований в общественных интересах может осуществляться без согласия субъекта ПД, если соблюдаются требования, установленные законодательством (например, по обезличиванию).	Оператору персональных данных необходимо получить согласие пациента на передачу медицинских данных любой стороне, не входящей в состав «медицинской команды».	Обработка данных для исследовательских и статистических целей осуществляется без отдельно данного согласия на обработку ПД. Согласие субъекта персональных данных при повторном использовании его данных не требуется.

	Израиль	США	Великобритания	Южная Корея	Европейский союз		
					Германия	Франция	Финляндия
Анонимизация данных	Минздрав Израиля выпустило три Информационных письма, которые разъясняют правила о защите медицинских персональных данных. Если иное не предусмотрено законом, персональные данные, подлежащие повторному использованию, должны быть обезличены.	Обезличенными должным образом данные считаются те данные, риск де-идентификации которых очень мал (т.е. для повторной идентификации субъекта требуется использование крайне трудоемких и дорогостоящих методов и процедур), HIPAA.	Данные о состоянии здоровья, обрабатываемые в научных, исследовательских или в статистических целях, должны пройти процедуру анонимизации . •Специальные требования к анонимизации предусмотрены в Руководстве об обезличивании медицинских данных.	После получения письменного согласия субъекта ПД на обработку данных для проведения исследования, а также для их обезличивания Комитет по биоэтике может отказать в одобрении заявки на обработку медданных.	Данные о состоянии здоровья, обрабатываемые в научных, исследовательских или в статистических целях, должны пройти процедуру анонимизации (раздел 27 (3) Закона о защите данных). •Специальные требования к анонимизации предусмотрены в Руководстве о медицинских данных опубликованном Министерством экономики Германии.	Данные о состоянии здоровья, обрабатываемые в научных, исследовательских или в статистических целях, должны пройти процедуру анонимизации.	Закон о повторном использовании медданных расширил сферу доступности таких данных, включив в нее, помимо традиционных исследований и статистики, также области управления, развития, инноваций, образования, планирования, а также управления и надзора. Данные предоставляются в обезличенном или псевдинимизированном виде.

	Израиль	США	Великобритания	Южная Корея	Европейский союз		
					Германия	Франция	Финляндия
Правовой режим анонимизированных данных	Разрабатываемый законопроект, регулирующий порядок анонимизации данных, требует удаление всех идентифицирующих элементов.	HIPAA считает де-идентифицированную информацию с сохранением кода, позволяющего повторную идентификацию, обезличенной информацией, на которую не распространяются требования по защите персональных данных.	Анонимизация (необратимое обезличивание) персональных данных признается труднодостижимой на практике и может снизить полезность соответствующего набора данных. Простое удаление идентификаторов может привести к получению псевдонимизированных данных, которые считаются персональными данными и составляют объект регулирования законодательства о защите персональных данных.				
			В случае сохранения кода информация является персональной.				
Совместимость, переносимость данных	В информационных письмах Орган по надзору в сфере ИТ рекомендует операторам обеспечить возможность субъекта ПД передать свои данные от одного оператора к другому.	HIPAA предоставляет пациентам право на доступ к персональным медданным, собранным и хранящимся в медорганизациях. Однако при этом в HIPAA никак не раскрывается вопрос передачи данных от одного оператора к другому.	Установлены требования к обеспечению переносимости данных.	В PIPA отсутствуют положения, регулирующие право субъекта ПД на переносимость данных.	В GDPR установлены требования к обеспечению переносимости данных (data portability).		
Аналоги ЕГИСЗ, МИС	+	+	+	+	+	+	+
Дата-посредники в медицинской отрасли	+ MDClone ADAMS Platform	+ Luna DNA, Amazon HealthLake и др.	+ Genomics England	+ Macrogen	+ Research Data Centre at the BfArM	+ Health Data Hub	+ Findata

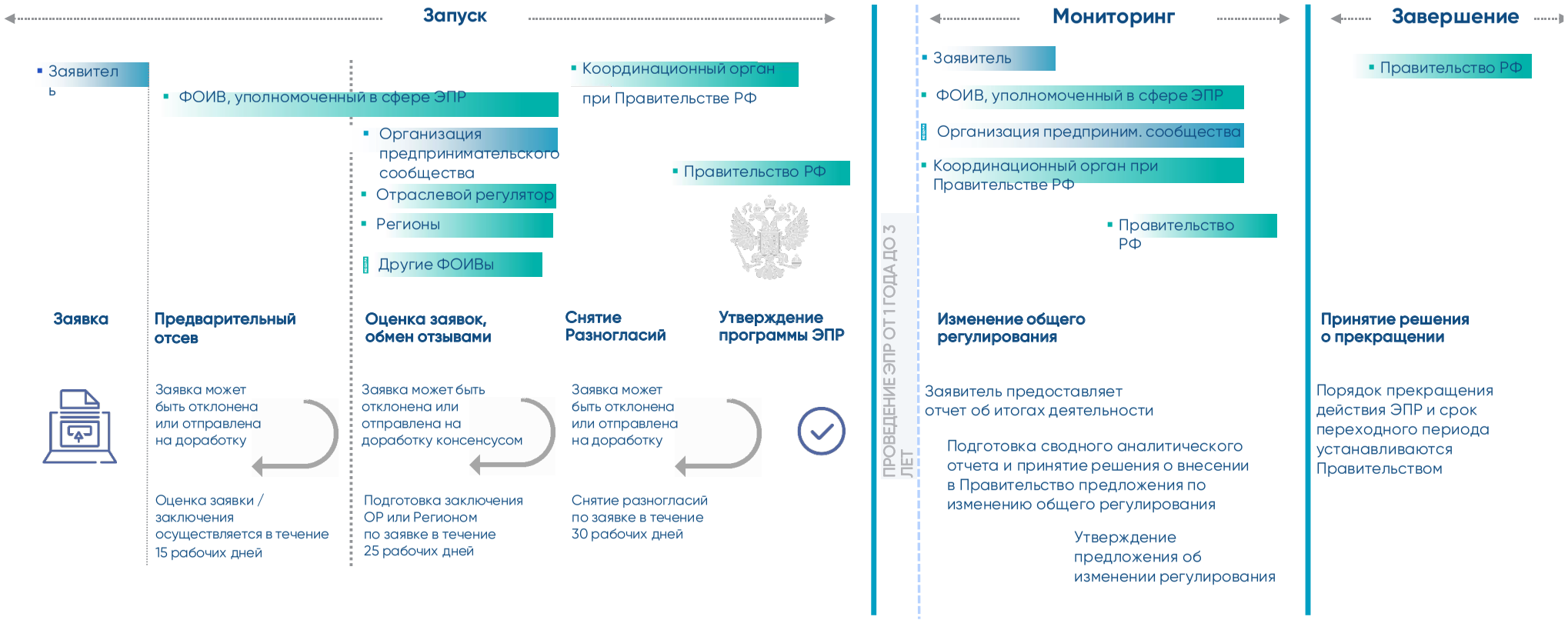
4. Практические примеры внедрения технологий искусственного интеллекта в медицине: экспериментальные правовые режимы

Для целей создания механизма апробации инновационного регулирования в паспорте федерального проекта «Нормативное регулирование цифровой среды» национальной программы «Цифровая экономика Российской Федерации» обозначена необходимость законодательного регулирования вопросов создания и функционирования особых правовых режимов в условиях цифровой экономики – так называемых «цифровых песочниц». Во исполнение данного мероприятия 8 января 2021 года вступил в силу Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых технологий». Запуск «цифровых песочниц» позволит дата-посредникам и другим участникам тестировать новые проекты и технологии обмена данными в безопасной и контролируемой среде, получая по итогам запуска экспериментального правового режима рекомендации для имплементации общего регулирования.

«Цифровая песочница» подразумевает создание особого правого режима по тестированию правовой «гипотезы» перед приданием ей общеобязательного характера и /или отмену действующих нормативных требований, которые мешают внедрению инноваций (например, пункт 2 статьи 5 Федерального закона «О персональных данных»). В отличие от снятия регуляторных барьеров, касающихся всех субъектов экономической деятельности, «цифровая песочница» носит временный характер и может быть ограничена субъектным составом.

Максимальный срок действия «цифровых песочниц» – три года; по истечении данного срока, при подтверждении безопасности апробируемого механизма, правила «регуляторной песочницы» можно масштабировать на всю страну, трансформировав в общее регулирование.

Схема установления ЭПР по 258-ФЗ



Экспериментальный правовой режим — это:

- Ограниченный **состав участников**
- Ограниченное **время**
- Ограниченная **территория** (как правило)

4.1 RWE-исследования

RWE-исследования: получение доказательств в условиях рутинной клинической практики позволяет участникам системы здравоохранения провести глубинный анализ эффективности терапии на основании полученных данных о клинических и экономических исходах в реальной практике ведения пациентов.

От первого лица

Виталий Омельяновский
Генеральный директор Центра экспертизы и контроля качества медицинской помощи Минздрава России, д.м.н., профессор

Во всем мире данные реальной клинической практики (РКП) становятся одним из инструментов оценки медицинских технологий для принятия решений, касающихся возможности их применения в клинической практике и целесообразности включения в систему государственного финансирования. Текущий уровень развития цифровизации здравоохранения в России позволяет собирать огромный массив медицинских данных, включая данные реальной клинической практики. Качество таких данных растет с каждым годом, что ставит вопрос о необходимости разработки подходов к их использованию и применению в текущей процедуре включения препаратов в перечни, при разработке федеральных проектов, в программах раннего доступа инновационных технологий, в разработке клинических рекомендаций.

По мнению экспертов, включение данных РКП уже частично реализуется в рамках клинических рекомендаций, однако данный вопрос требует серьезной проработки подходов и требований к проведению таких исследований и оценки их качества.

Одними из возможных источников данных реальной клинической практики могут выступать данные медицинской информационной системы (МИС) и структурированные электронные медицинские документы (СЭМД), агрегирующие первичные медицинские данные об оказанной медицинской помощи из медицинских информационных систем медицинских организаций и передающие их в Единую государственную информационную систему в сфере здравоохранения (ЕГИСЗ) и вертикально-интегрированные медицинские информационные системы (ВИМИС).

В настоящее время обсуждается установление экспериментально-правового режима для сбора и анализа данных РКП. Это очень важная инициатива, которая может стать дополнительным механизмом для повышения доступности инновационных технологий для пациентов.

Для RWE-исследований требуется обрабатывать большие массивы данных, а в силу действующего законодательства требуется получать письменные согласия субъектов персональных данных; необходимость получения тысяч письменных согласий является фактически непреодолимым барьером. Решение данной проблемы заключается в запуске «цифровых песочниц», механизм описанный в предыдущем разделе.

Препятствия: развитие персонализированной медицины крайне остро ставит вопрос о сборе данных реальной клинической практики. Для многих заболеваний, в первую очередь орфанных (малоисследованные заболевания), проведение качественных клинических исследований затруднено или невозможно, что приводит к дефициту достоверных и точных данных. В таких случаях альтернативой или единственным источником данных является реальная клиническая практика.

Одними из факторов, препятствующих внедрению данных реальной клинической практики, являются, как отмечают эксперты, меньшая точность и достоверность таких

исследований, по сравнению с «классическими» клиническими исследованиями, золотым стандартом которых являются рандомизированные контролируемые исследования.

Так, компания Data MATRIX создает программные продукты для организации клинических исследований. Суть ее инициативного предложения экспериментального правового режима заключается в исследовании рутинной клинической практики (RWE), отражающей реальный практический опыт ведения пациентов с целью глубинного анализа эффективности терапии, лекарственных препаратов, методов диагностики и лечения.

Возможности новых технологий для ЭПР представители компании Data MATRIX показали на примере собранных обезличенных данных пациентов с диагнозом «рак молочной железы». Для оценки эффективности лекарств компания предлагает использовать обезличенные данные пациентов. Технологии искусственного интеллекта помогут оценить эффективность лекарственной терапии и скорректировать лечение, оценить вероятность выздоровления при смене препаратов.

От первого лица

Алексей Лолейт
Заместитель генерального директора по стратегии и развитию продукта «Дата МАТРИКС»

Цифровизация и развитие технологий обработки данных и ML уже позволяют в глобальном масштабе анализировать данные, относящиеся к состоянию здоровья пациента и к процессу оказания медицинской помощи, полученные из обезличенных электронных медицинских карт. Анализ данных реальной клинической практики (RWD) — это способ изучить эффективность и переносимость терапии у фактической популяции российских пациентов, возможность получать доказательства для улучшения методов лечения, профилактики и диагностики, выявлять закономерности, которые невозможно идентифицировать в классических клинических исследованиях.

С шестидесятых годов рандомизированные контролируемые исследования (RCTs) рассматриваются как золотой стандарт доказательств в медицине. Однако, такие исследования с их критериями включения/невключения определенных когорт пациентов не в полной мере отражают все нюансы реальной практики и не охватывают различные субпопуляции пациентов, особенно пациентов в зоне риска. Исследования реальной клинической практики (RWE) позволяют расширить аналитику и получать доказательства эффективности лечения пациентов различных демографических групп и пациентов с сопутствующими заболеваниями, оценить исход терапии в реальной популяции пациентов.

RWE несут практическую ценность для всех участников системы здравоохранения как со стороны регуляторов и производителей, так и со стороны врачебного и пациентского сообщества. В международной практике потенциал доказательств RWE используют в следующих направлениях:

- Разработка, изучение и регистрация лекарственных препаратов;
- Пострегистрационная безопасность и пострегистрационная эффективность, включая изменения в инструкции по применению уже зарегистрированных препаратов: добавление или пересмотр показаний, изменение дозировки и схем применения, добавление новых пациентов, в том числе детей и т.д.;
- Формирование клинических рекомендаций;

- Формирование подходов к возмещению затрат, фармакоэкономика и оценка технологий здравоохранения.

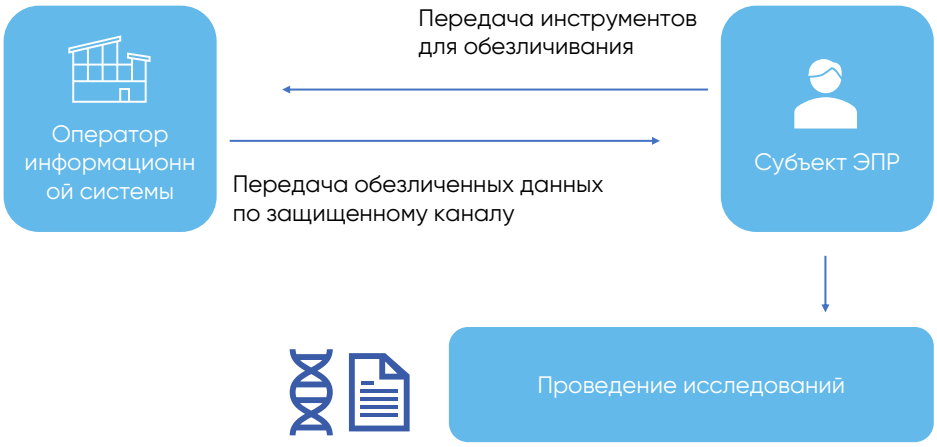
Анализ RWD может помочь клиническому сообществу лучше понять результаты терапии и то, как работают методы лечения и лекарственные препараты в реальной жизни, дает возможность получать информацию об особых категориях пациентов, незадействованных в традиционных КИ, более того знания о таких пациентах - ключ к разработке новых лекарственных препаратов.

Практикующие врачи и пациенты могут использовать системный анализ RWE для принятия более информированных решений о выборе стратегии лечения, прогнозирования эффективности терапии.

Фарминдустрия может подтверждать эффективность препаратов, проводя комплексную оценку эффективности препарата, что особенно важно в случае орфанных заболеваний, мутаций в онкологии. Результаты RWE исследований также могут быть использованы для планирования будущих клинических исследований. На практике запуск RWE исследования может помочь в гораздо более короткие сроки получить опорные данные по сравнению с альтернативными традиционными подходами.

Данные реальной клинической практики важны для системы здравоохранения и принятия регуляторных решений в отношении регистрации лекарственных препаратов, нужны для формирования клинических рекомендаций и при определении подходов к возмещению стоимости лекарственной терапии.

Схема ЭПР Data MATRIX



Параметры ЭПР Data MATRIX

Сбор и дальнейшая обработка данных без согласия субъектов персональных данных, при соблюдении следующих условий:

- **Специальное программное обеспечение для обезличивания.** Данные должны быть обезличены методом изменения состава или семантики на стороне лечебно-

профилактического учреждения с использованием программного обеспечения для обезличивания, предоставленного компанией Data MATRIX.

- **Создание системы ИТ-безопасности.** Информационная система, в которой будут аккумулироваться данные, должна иметь наивысший класс защиты по Приказу ФСТЭК № 17[112], а также соответствовать иным требованиям законодательства.

- **Защищенная передача данных.** При передаче обезличенных данных из лечебно-профилактического учреждения в Data MATRIX должен использоваться VPN, сертифицированный ФСБ.

- **Регулярная отчетность.** Субъекты «цифровой песочницы» должны каждые полгода, а также в самом конце функционирования «цифровой песочницы» предоставлять отчеты о своей деятельности.

Какие данные планируются обрабатывать:

- демографические;
- антропометрические;
- о диагнозе;
- об анамнезе заболевания и жизни;
- о дате и причине смерти;
- о визитах пациента к врачу;
- о медицинской организации;
- об обследованиях;
- о лабораторных тестах / физиологических показателях;
- о проведенных процедурах;
- о назначении лекарственных средств.

Международный опыт

В Великобритании компания Genomics England является дата-депозитарием, который собирает данные о геноме человека для исследовательских целей в рамках проекта «100 000 геномов». Компания секвенирует геномные данные людей (исследует всю последовательность ДНК человека) с редкими заболеваниями или раком в исследовательских или медицинских целях[113].

В США геномно-медицинский исследовательский стартап Luna DNA использует технологию блокчейн для безопасного хранения данных и выплачивает вознаграждение субъектам персональных данных за предоставление их медицинской информации собственной криптовалютой – «луна коинами», которая имеет реальную денежную стоимость. Luna DNA – это платформа для исследований в области здравоохранения, к которой может присоединиться любой желающий, поделиться своими медицинскими данными и в обмен получить вознаграждение[114].

Создаваемая в ходе «цифровой песочницы» инфраструктура станет востребованным инструментом для всех участников системы здравоохранения. Сформированная экспертная группа при АНО «Цифровая экономика» уже рассмотрела и сформировала комментарии к проекту программы экспериментального правого режима для больших массивов данных в медицине, которые будут учтены при дальнейшем рассмотрении инициативы. На момент написания аналитического отчета проект проходит один из критически значимых этапов – согласование по кибербезопасности и защищенности каналов для обеспечения безопасности обрабатываемых данных и соблюдения баланса между рисками и важностью инноваций по отношению к интересам граждан.

Опыт Южной Кореи

В Южной Корее государственная информационная система медицинского страхования и информационные системы медицинских организаций накапливают большие массивы медицинских данных (уровень внедрения электронных медицинских карт (EMR) в стране превышает 90%[115]). Такие данные могут быть использованы для профилактики развития медицинских заболеваний и повышения производительности и эффективности исследований при разработке лекарственных препаратов.

Недавние поправки в закон Южной Кореи о защите персональных данных (PIPA)[116] позволяют обрабатывать и передавать обезличенные данные без предварительного согласия пациента. Однако на протяжении многих лет осуществить сбор биологических образцов и медицинских данных, необходимых для проведения исследований, было практически невозможно из-за барьеров, заложенных в законе о биоэтике и безопасности[117].

Так, закон о биоэтике и безопасности[118] все еще запрещает использовать и обрабатывать генетические данные и биоматериалы в исследовательских и коммерческих целях, если только субъект данных или донор не дали на это письменное согласие. Такое согласие должно также пройти оценку Комитетом по биоэтике[119].

Также конкретная цель исследования, для которого осуществляется сбор данных, должна быть указана в форме письменного согласия на передачу и обработку персональных данных, что делает невозможным повторную обработку данных для иных целей (например, для других аналогичных исследований). Следует отметить, что разработчику/исследователю необходимо получить письменное согласие субъекта персональных данных также при передаче биологических или медицинских данных другим исследователям или в банк данных, а также для обезличивания таких данных. Однако поиск субъекта персональных данных для получения письменного согласия на обработку персональных данных каждый раз, когда биоматериал или медицинские данные используются, передаются или обезличиваются в исследовательских целях, – процесс дорогой и непрактичный. Более того, даже после получения письменного согласия субъекта персональных данных на обработку данных для проведения исследования, а также для их обезличивания Комитет по биоэтике может отказать в одобрении заявки на обработку медицинских данных[120].

По мнению экспертов из Южной Кореи, персональные данные необходимы разработчикам для проведения исследований в целях создания новых лекарств и проведения ранней диагностики[121]. Состояние здоровья, реакция на лекарства, погодные условия, состояние окружающей среды в регионе, где проживает пациент, – все это может повлиять на его здоровье, а для того, чтобы использовать эту

информацию, необходимо обработать персональные данные о месте жительства пациента и его ежедневный маршрут[122].

В 2019 году в Южной Корее принят ряд нормативных правовых актов, регулирующих «цифровые песочницы»[123], которые позволяют субъектам ЭПР временно отступать от действующих норм законодательства для внедрения и коммерциализации новых технологий и бизнес-моделей в Южной Корее. «Цифровые песочницы» могут быть созданы сроком как минимум на два года и продлены еще на один год. Регулятор вместе с участниками эксперимента изучает, как работает новая технология и нужно ли менять регулирование. Решение о масштабировании «правовой рамки» принимается только по завершении экспериментального правового режима.

В 2019 году Правительство Южной Кореи запустило «цифровую песочницу»[124] по разработке и использованию генетических тестов (DTC, direct to consumer или коробочные тесты), позволяющую временно отступать от действующих норм закона о биоэтике и безопасности (проект Macrogen, Inc)[125]. В рамках «цифровой песочницы»[126] компании вправе проводить исследования в сфере генетического тестирования (DTC) на 2000 граждан, проживающих в городе Сонгдо. Если эксперимент окажется удачным и субъекты ЭПР докажут безопасность разработанного DTC для лиц, страдающих серьезными заболеваниями, правительство рассмотрит вопрос об изменении общего регулирования. К таким заболеваниям программа «цифровой песочницы» относит: хронические заболевания, такие как гипертония и диабет 2 типа, некоторые виды рака и заболевания людей старших возрастных групп (гериатрические заболевания), такие как деменция.

Используя геномную информацию пациента, врачи теперь могут составлять индивидуальные планы лечения с учетом анализа генетических биомаркеров человека при определенных заболеваниях – с помощью DTC[127].

Напомним, в соответствии с российским законодательством геномные данные тоже попадают под понятие «врачебной тайны»: геномные данные составляют медицинскую тайну и для их обработки необходимо получение с пациентов информированного согласия[128].

Чон-Сун Сео, представитель компании Macrogen, заявляет, что «конечная и долгосрочная цель данного проекта – исследовать геномные данные на благо человечества и дать людям информацию о своем собственном геноме. Микробиом человека (триллионы микробов, живущих внутри и вне организма) и его влияние на здоровье и болезни – это развивающаяся область. Изучение взаимодействия между микробиомом человека, генотипом и окружающей средой открывает новые возможности в точной медицине – в частности, геномное влияние на формирование полезных бактерий человека. Собирая такие данные в централизованную базу данных, компания Macrogen надеется создать наборы больших массивов данных для их эффективного использования в Азиатско-Тихоокеанского регионе – самого быстрорастущего в мире рынка точной медицины стоимостью 20,9 миллиарда долларов США к 2023 году»[129].

4.2 Проект-маяк «Персональные медицинские помощники»

От первого лица

Антон Кокин
Руководитель проектного офиса «Медицина», АО «Объединенная приборостроительная корпорация»

Использование телекоммуникационных технологий для оказания медицинской помощи на расстоянии кажется достаточно простым методом, учитывая то, что у большинства людей есть доступ к основным телекоммуникационным технологиям, таким как телефоны, интернет и компьютеры. Но для многих решений в области дистанционного мониторинга требуется больше ресурсов, чем минимальные основы дистанционного взаимодействия. Снизить риски такого взаимодействия, унифицировать и реализовать все преимущества таких технологий является задачей Стратегической инициативы «Персональные медицинские помощники».

Реализация инициативы Персональные медицинские помощники позволит понять принципы закрытия «серой зоны» удалённого взаимодействия между пациентами и врачами для всех требуемых видов нозологий, обеспечить врачей точными валидированными первичными данными с соблюдением базового баланса информационной безопасности.

АО «Объединенная приборостроительная корпорация» разработало программу экспериментального правового режима (ЭПР) в области медицины, предполагающую использование носимых электронных устройств для дистанционного наблюдения за здоровьем пациентов.

Такая возможность будет стимулировать расширение рынка устройств мониторинга и ПО для контроля состояния здоровья, а также более быстрый переход к пилотированию таких изделий. Учитывая крайне малое число имеющихся на рынке устройств и решений, стимулирование их выхода на рынок является важнейшей задачей.

Согласно программе «цифровая песочница» направлена на расширение возможностей медицинских технологий за счет «дистанционного наблюдения за состоянием здоровья граждан с использованием медицинских изделий и носимых устройств, не являющихся зарегистрированными в установленном порядке медицинскими изделиями» (аксессуары и иные форм-факторы (браслеты, фитнес-трекеры)).

Носимые устройства собирают и передают связанную со здоровьем информацию, которую можно было бы использовать как дополнительный источник данных при профилактике заболеваний, в том числе артериальной гипертензии и диабета.

Описание «цифровой песочницы»:

1. Устройство регистрируется на платформе ПМП («персональных медицинских помощников»).

2. После регистрации на платформе медицинский работник проверяет «персонального медицинского помощника» (далее – ПМП) и выдает устройство пациенту для применения.

3. Показания с прибора поступают в МИС в режиме реального времени.

4. Врач принимает решение на основе показаний используемого глюкометра, в том числе с использованием системы поддержки принятия врачебных решений.

Регуляторный барьер, который планируется нивелировать:

Отсутствует техническое регулирование для устройств ПМП и защищенного канала связи при передаче сигнальной информации и смс-уведомлений.

Решение:

Изъятие из Постановления Правительства Российской Федерации от 12 апреля 2018 г. № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями» нормы, регулирующей обеспечению защищенного канала связи при передаче сигнальной информации и смс-уведомлений пользователям устройств «персональных медицинских помощников».

Корреспондирующее изъятие для выработки технического регулирования – опытная эксплуатация ГИС по Постановлению Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

Опыт Южной Кореи

Так, в Южной Корее запущена «цифровая песочница», которая позволяет обмениваться данными с носимых устройств в сфере здравоохранения. Например, умные часы способны отправлять электрокардиограмму (детальную и ничем незаменимую информацию о состоянии сердца) владельца устройства врачу при записи каких-либо отклонений[130].

Носимые устройства vs медицинские устройства. В Южной Корее также предпринимаются шаги в области сертификации и использования носимых устройств в здравоохранении. Так, Корейское министерство безопасности пищевых продуктов и медикаментов (MFDS) проводит сертификацию (регистрацию) носимых устройств в качестве медицинских изделии. Например, приложение для измерения артериального давления и смарт-часы на базе этого приложения, должны быть зарегистрированы в качестве медицинского изделия.

Таким образом, в Южной Корее носимые устройства признаны медицинскими устройствами и проходят сертификацию.

Регулирование персональных данных. Согласно Закону о защите персональных данных (PIPA)[131] любая личная информация (запись голоса, фотография, виртуальное изображение, ИНН и т. д. – в общем, все, что может идентифицировать человека как физическое лицо) считается персональными данными. Производители носимых устройств должны защищать персональные данные пользователей в соответствии с теми же принципами, которые установлены в PIPA; в противном случае будет наложен штраф.

Опыт Германии

Закон Германии о цифровом здравоохранении вступил в силу 19 декабря 2019 года и закрепил понятие «приложение по рецепту» (медицинское приложение),т. е. цифровое медицинское приложение для оказания медицинской помощи (на немецком языке: digitale Gesundheitsanwendungen, далее DiGA). В августе 2020 года Федеральный институт лекарств и медицинских изделий (Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM) выпустил Информационное письмо[132], в котором установлены требования к производителям DiGA, чтобы сделать DIGA доступными для более чем 73 миллионов страхователей обязательного медицинского страхования Германии.

DiGA – это приложения для мониторинга состояния здоровья. Для того чтобы квалифицировать приложение в качестве DiGA, приложения, помеченные меткой CE как медицинские устройства с низким уровнем риска класса 1 и 2a[133], должны успешно пройти ускоренный процесс оценки BfArM. BfArM оценивает приложение с точки зрения его безопасности, функциональности, защиты данных, информационной безопасности, медицинской эффективности, интероперабельности, качества данных, положительного воздействия приложения на здоровье[134].

Для реализации проекта DiGA немецкие законодатели разработали новую правовую основу: Закон о цифровом здравоохранении, принятый в декабре 2019 года. Согласно новому закону 73 миллиона немцев, оформившие обязательное медицинское страхование (примерно 90% от общей численности населения), теперь вправе использовать DiGA при условии, что у пациентов уже есть рецепт или подтвержденный диагноз.

Выводы

Указом Президента России № 490 от 10.10.2019 была утверждена Национальная стратегия развития искусственного интеллекта (ИИ) в Российской Федерации на период до 2030 года, направленная на то, чтобы Россия стала одной из стран – лидеров в области ИИ. Одним из ключевых направлений стратегии является развитие рынка программных продуктов на основе ИИ для здравоохранения.

Следует отметить, что любая страна с надежной базой медицинских данных в сочетании с наличием выдающихся технологических решений может претендовать на статус страны – лидера в мире искусственного интеллекта. Примеров таких технологических решений в России много: Botkin.ai, Care Mentor AI, Celsus, Webiomed, Sapia, «Инсилико», Data MATRIX и др. На сегодняшний день также существует ЕГИСЗ, РМИС – информационные системы, аккумулирующие различные типы медицинских данных. Получается, что осталось достроить этот «мостик» между разработчиками технологических решений в сфере медицины и набором медицинских данных, предоставив доступ к таким обезличенным данным в защищенном контуре. Для этого необходимо снять ряд регуляторных барьеров, среди которых: отсутствие возможности использования оператором персональных данных ранее собранных данных для иных целей при наличии согласия субъекта персональных данных, необходимость получения письменных согласий на обработку персональных данных пациентов, даже если такие данные будут обезличены, а также отсутствие доступа к большому объему обезличенных медицинских данных.

По мере того как мир движется к эпохе цифровых технологий и платформ в области здравоохранения, необходимо также оценить то, насколько тесно могут сосуществовать принципы свободного обмена данными и защиты персональных данных. В аналитическом отчете обсуждены главные вызовы и ответные меры в России и за рубежом (представлен опыт стран ЕС, Азии, а также Великобритании и США).

Так как одной из целей свободного обмена данными пациентов является развитие технологий в области ИИ при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений), интерес пациентов должен быть защищен в правовой форме, т. е. через введение института дата-посредничества. Такое регулирование корреспондирует иностранным подходам (Южная Корея, Германия), где в силу строгости регулирования персональных данных (полный контроль субъекта персональных данных над своими данными; обработка медицинских данных чаще всего осуществляется с согласия пациента) был имплементирован институт дата-посредничества в медицине путем запуска «цифровых песочниц». Наряду с этим предлагается исключить в рамках «цифровых песочниц» необходимость получения письменных согласий на обработку персональных данных пациентов в случае, если такие данные будут обезличены.

Отметим, что страны с более консервативным подходом к регулированию персональных данных, аналогичным российскому подходу, стремятся сохранить баланс между безопасностью данных, открытостью данных и правами граждан на свои медицинские данные. Такой баланс достигается путем внедрения института дата-посредников, учитывающего интересы органов власти (новые методики обезличивания, обеспечивающие минимизацию деидентификации), граждан (закрытый контур и защита от утечек), бизнес-сообщества/разработчиков технологических решений (доступ

к большим наборам данным), врачей (снятие барьеров для введения решений на основе ИИ при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений)).

В связи с этим представляется необходимым создать такой надежный механизм управления данными, как дата-посредники, для того чтобы воспользоваться преимуществами аналитики больших массивов данных в медицине: при принятии решений о диагностике и лечении на основании предложения алгоритма (системы поддержки принятия врачебных решений), для проведения медицинских исследований и развития технологий в области ИИ или для формирования комплексной оценки методов диагностики, лекарственного и нелекарственного лечения, профилактики и реабилитации.

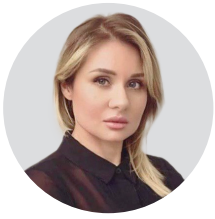
Таким образом, для того чтобы максимально эффективно использовать медицинские данные для развития решений на основе ИИ, предлагается запустить механизм «регуляторных песочниц», который позволит апробировать и внедрить безопасный и свободный обмен медицинскими данными для исследовательских целей путем внедрения института дата-посредничества.

Авторы

Римма Чичакян
Руководитель проектов направления «Эффективное регулирование», АНО «Цифровая экономика»

Борис Зингерман
Генеральный директор Ассоциации НБМЗ и руководитель направления цифровой медицины компании ИНВИТРО
Позиция автора на стр. 18

Марина Ляшенко
Эксперт по финансовому рынку, Ассоциация Финтех
Позиция автора на стр. 32



Ольга Гребнева
Руководитель направления, Лаборатория финтех и инноваций САО «ВСК»
Позиция автора на стр. 48, 50

Виталий Омельяновский
Генеральный директор Центра экспертизы и контроля качества медицинской помощи Минздрава России, д.м.н., профессор.
Позиция автора на стр. 60

Алексей Лолейт
Заместитель генерального директора по стратегии и развитию продукта «Дата МАТРИКС»
Позиция автора на стр. 61

Антон Кокин
Руководитель проектного офиса «Медицина», АО «Объединенная приборостроительная корпорация»
Позиция автора на стр. 66

Редакционная коллегия

Карен Казарян
Директор по аналитике, АНО «Цифровая экономика»

Примечания

1 Statista. (2019, October). Global digital population as of October 2019. Retrieved from Statista: https://www.statista.com/statistics/617136/digital-population-worldwide/

2 IQVIA. The growing value of digital health, evidence and impact on human health and the healthcare system, 2017. https://www.iqvia.com/insights/the-iqvia-institute/reports/the-growingvalue-of-digital-health

3 Big Data Analytics in Healthcare. (2019). Germany: Springer International Publishing. P. 3–4.

4 https://www.bu.edu/cise/research-areas/computational-biology-medicine/

5 Health Data Research UK, "Our Hubs", https://www.hdruk.ac.uk/helping-with-health-data/health-data-research-hubs/

6 Health Data Research UK, "Improving UK Health Data: Impact from Health Data Research Hubs", 2021. P. 10–13 // https://www.hdruk.ac.uk/wp-content/uploads/2021/04/Improving-UK-Health-Data-Impacts-from-Health-Data-Research-Hubs_compressed.pdf

7 Москва пополнила цифровую библиотеку данных для тестирования нейросетей в медицине. https://www.mos.ru/news/item/114636073/

8 https://www.ibm.com/products/watson-imaging-patient-synopsis

9 https://aws.amazon.com/about-aws/whats-new/2020/12/introducing-amazon-healthlake-to-make-sense-of-healthdata

10 Kwong, A, Hameed, B, Syed, S, et al. Machine learning to predict waitlist dropout among liver transplant candidates with hepatocellular carcinoma. Cancer Med. 2022; 11: 1535–1541. doi:10.1002/cam4.4538

11 Stefano A. Bini, Romil F. Shah, Ilya Bendich, Joseph T. Patterson, Kevin M. Hwang, Musa B. Zaid,

Machine Learning Algorithms Can Use Wearable Sensor Data to Accurately Predict Six-Week Patient-Reported Outcome Scores Following Joint Replacement in a Prospective Trial, The Journal of Arthroplasty, Volume 34, Issue 10, 2019, Pages 2242–2247.

12 Ross MK, Wei W, Ohno-Machado L. "Big data" and the electronic health record. Yearb Med Inform. 2014;9:97–104.

13 Saravia, E., Chang, C., De Lorenzo, R., & Chen, Y. (2016). MIDAS: mental illness detection and analysis via social media. Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 1418–1421

14 Roy, A., Nikolitch, K., McGinn, R., Jinah, S., Klement, W., & Kaminsky, Z. (2020). A machine learning approach predicts future risk to suicidal ideation from social media data. NPJ Digital Medicine, 3(1), 78–78. https://doi.org/10.1038/s41746-020-0287-6

15 Roy, A., Nikolitch, K., McGinn, R., Jinah, S., Klement, W., & Kaminsky, Z. (2020). A machine learning approach predicts future risk to suicidal ideation from social media data. NPJ Digital Medicine, 3(1), 78–78. https://doi.org/10.1038/s41746-020-0287-6

16 Liang, Y., Zheng, X., & Zeng, D. (2019). A survey on big data-driven digital phenotyping of mental health. Information Fusion, 52, 290–307. https://doi.org/10.1016/j.inffus.2019.04.001

17 Liang, Y., Zheng, X., & Zeng, D. (2019). A survey on big data-driven digital phenotyping of mental health. Information Fusion, 52, 290–307. https://doi.org/10.1016/j.inffus.2019.04.001

18 Liang, Y., Zheng, X., & Zeng, D. (2019). A survey on big data-driven digital phenotyping of mental health. Information Fusion, 52, 290–307. https://doi.org/10.1016/j.inffus.2019.04.001

19 Wongkoblap, A., Vadillo, M., & Curcin, V. (2017). Researching Mental Health Disorders in the Era of Social Media: Systematic Review. Journal of Medical Internet Research, 19(6), https://doi.org/10.2196/jmir.7215. P. 228.

20 Ibid.

21 Gjoreski, M., Luštrek, M., Gams, M., & Gjoreski, H. (2017). Monitoring stress with a wrist device using context. Journal of Biomedical Informatics, 73, 159–170. https://doi.org/10.1016/j.jbi.2017.08.006

22 Beam, A., & Kohane, I. (2018). Big Data and Machine Learning in Health Care. JAMA : the Journal of the American Medical Association, 319(13), 1317–1318.

23 Kamran Ul haq, A., Khattak, A., Jamil, N., Naeem, M., & Mirza, F. (2020). Data Analytics in Mental Healthcare. Scientific Programming, 2020, 1–9.

24 Kamran Ul haq, A., Khattak, A., Jamil, N., Naeem, M., & Mirza, F. (2020). Data Analytics in Mental Healthcare. Scientific Programming, 2020, 1–9.

25 Shatte, A., Hutchinson, D., & Teague, S. (2019). Machine learning in mental health: a scoping review of methods and applications. Psychological Medicine, 49(9), 1435.

26 Menear M., Blanchette M-A., Demers-Payette O., Roy D. (2019). A framework for value-creating learning health systems. Health Research Policy and Systems. 17. Friedman C., Allee N., Delaney B., Flynn A., Silverstein J., Sullivan K., Young K. (2016).The science of Learning Health Systems: Foundations for a new journal. Learning Health.

27 Постановление Правительства Российской Федерации от 5.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения» (утр. силу).

28 Постановление Правительства Российской Федерации от 5.05.2018 № 555 «О единой государственной информационной системе в сфере здравоохранения» (утр. силу).

29 Постановление Правительства РФ от 09.02.2022 N 140 «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»).

30 Федеральный закон от 27.12.2002 № 184-ФЗ (ред. от 02.07.2021) «О техническом регулировании».

31 Методические рекомендации по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО) (утв. Министерством здравоохранения РФ 1 февраля 2016 г.)

32 Deloitte. Wearable technology in health care: Getting better all the time. December 2021. // https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2022/wearable-technology-healthcare.html

33 Deloitte. Wearable technology in health care: Getting better all the time. December 2021. // https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2022/wearable-technology-healthcare.html

34 The General Data Protection Regulation (EU) (GDPR). 2016.

35 The United Kingdom General Data Protection Regulation (UK-GDPR)

36. Nathalie Moreno, Johanna Saunders, Annabelle Gold-Caution, Lydia Loxham. Balancing the Power of Data in Digital Health Innovation. ICLG. // https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiun5LZmuz6AhXFtYsKHVdNB8oQFnoECBIQQ&url=https%3A%2F%2Ficlg.com%2Fpractice-areas%2Fdigital-health-laws-and-regulations%2F4-balancing-the-power-of-data-in-digital-health-innovation&usg=AOvVaw2J_K9K12-2-EpRMh1swxY_

37 Mostert M., Bredenoord A. L., Biesaart M. C. I. H., Van Delden J. J. M. (2016). Big Data in Medical Research and EU Data Protection Law: Challenges to the Consent or Anonymise Approach. Eur. J. Hum. Genet. 24 (7), 956–960. 10.1038/ejhg.2015.239

38 Jansen T. C., Kompanje E. J. O., Druml C., Menon D. K., Wiedermann C. J., Bakker J. (2007). Deferred Consent in Emergency Intensive Care Research: what if the Patient Dies Early? Use the Data or Not? Intensive Care Med. 33, 894–900. 10.1007/s00134-007-0580-8

39 Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., and Erlich, Y. (2013). Identifying Personal Genomes by Surname Inference. Science. P. 339, 321–324.

40 Sariyar, M., and Schlünder, I. (2016). Reconsidering Anonymization-Related Concepts and the Term "Identification" against the Backdrop of the European Legal Framework. Biopreservation Biobanking 14 (5). P. 367–374.

41 Ploem, M. C., Essink-Bot, M. L., and Stronks, K. (2013). Proposed EU Data Protection Regulation Is a Threat to Medical Research. BMJ 346, f3534.

42 Whitepaper Ver 1.1.0. Humanspace. // https://humanscape.hk/pdf/Humanscape_Whitepaper_EN_v1.1.0.pdf P. 10–13.

43 Whitepaper Ver 1.1.0. Humanspace. // https://humanscape.hk/pdf/Humanscape_Whitepaper_EN_v1.1.0.pdf P. 10–13.

44 Whitepaper Ver 1.1.0. Humanspace. // https://humanscape.hk/pdf/Humanscape_Whitepaper_EN_v1.1.0.pdf P. 10–13.

45 Подробнее см. Тренды совершенствования механизмов согласия в докладе https://c4ir.ru/reports/izmenenie-podhodov-k-oborotu-personalnyh-dannyh-pereosmyslenie-soglasiya-na-obrabotku/

46 Подробнее см. Тренды совершенствования механизмов согласия в докладе https://c4ir.ru/reports/izmenenie-podhodov-k-oborotu-personalnyh-dannyh-pereosmyslenie-soglasiya-na-obrabotku/

47 International Comparative Legal Guides. Digital Health. 2022. Third Edition. Contributing Editor: Roger Kuan Norton Rose Fulbright. P. 184.

48 Personal Information Protection Act (General Law) // https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=33

49 Bioethics And Safety Act. Act No. 16372, Apr. 23, 2019 // https://elaw.klri.re.kr/kor_service/lawView.do?lang=ENG&hseq=52559

50 Densen P. (2011). Challenges and opportunities facing medical education. Transactions of the American Clinical and Climatological Association, 122, 48–58.

51 European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

52 European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

53 Приказ Минздрава РФ от 07.09.2020 № 947н «Об утверждении порядка организации системы документооборота в сфере охраны здоровья в части ведения медицинской документации в форме электронных документов»

54 Cook JA, Collins GS. The rise of big clinical databases. Br J Surg. 2015;102:e93–101.

55 Weiskopf NG, Weng C. Methods and dimensions of electronic health record data quality assessment: enabling reuse for clinical research. J Am Med Inform Assoc. 2013;20(1):144–151. doi: 10.1136/amiajnl-2011-000681.

56 Guidelines 05/2020 on consent under Regulation 2016/679 // https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf Ch. 4.

57 п. 52 Преамбулы GDPR

58 Assessment of the EU Member States' rules on health data in the light of GDPR // European Commission, 2021 https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf P. 42–57.

59 Guidelines 05/2020 on consent under Regulation 2016/679 // https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

60 Ibid.

61 Assessment of the EU Member States' rules on health data in the light of GDPR // European Commission, 2021 https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf. P. 42–57.

62 Assessment of the EU Member States' rules on health data in the light of GDPR // European Commission, 2021 https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf. P. 42–57.

63 Assessment of the EU Member States' rules on health data in the light of GDPR // European Commission, 2021. https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf P. 42–57.

64 Ibid.

65 Ibid.

66 European Data Protection Supervisor (2020). A Preliminary Opinion on data protection and scientific research. European Commission. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

67 KNAW (2018) Netherlands Code of Conduct Integrity. https://www.knaw.nl/shared/resources/actueel/bestanden/netherlands-code-of-conductfor-research-integrity-2018-uk

68 Assessment of the EU Member States' rules on health data in the light of GDPR // European Commission, 2021 https://ec.europa.eu/health/sites/default/files/ehealth/docs/ms_rules_health-data_en.pdf P. 42–57.

69 Heckmann D., Scheurer M. (2021). "Datenschutzrecht," in Praxiskommentar Internetrecht. Juris. Editors Heckmann D., Paschke A.

70 Shabani M., Borry P. (2018). Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation. Eur. J. Hum. Genet. 26, 149–156.

71 Kindt E., Fontanillo Lopez C. A., Czarnocki J., Kanevskaia O., Herveg J. (2021). Study on the Appropriate Safeguards Required under Article 89(1) of the GDPR for the Processing of Personal Data for the Scientific Research. Prep. by Milieu under lead KU-Leuven under Contract No EDPS/2019/02-08 benefit EDPB

72 Slokenberga S., Tzortzatou O., Reichel J. (2021). GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation across Europe. Cham, Switzerland: Springer Nature, 434.

73 Bak M. A. R., Ploem M. C., Ateşyürek H., Blom M. T., Tan H. L., Willems D. L. (2020). Stakeholders' Perspectives on the Post-mortem Use of Genetic and Health-Related Data for Research: a Systematic Review. Eur. J. Hum. Genet. 28 (4), 403–416.

74 Ministry of Social Affairs and Health, Finland (2019). Act on the Secondary Use of Health and Social Data.

75 Aula V. (2019). Institutions, Infrastructures, and Data Friction-Reforming Secondary Use of Health Data in Finland. Big Data Society 6 (2).

76 Vrijenhoek T., Tonisson N., Kääriäinen H., Leitsalu L., Rigter T. (2021). Clinical Genetics in Transition-A Comparison of Genetic Services in Estonia, Finland, and the Netherlands. J. Community Genet. 12 (2), 277–290.

77 Biobank Act (2012). Ministry of Social Affairs and Health, Finland. Biobank Act; 688.

78 European Commission (2019). Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Jormanainen V., Parhiala K., Niemi A., Erhola M., Keskimäki I., Kaila M. (2019). Half of the Finnish Population Accessed Their Own Data: Comprehensive Access to Personal Health Information Online Is a Corner-Stone of Digital Revolution in Finnish Health and Social Care. Finn. J. eHealth Welf. 11 (4). 10.23996/fjhw.83323

79 European Commission (2019). Ethics Guidelines for Trustworthy AI. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Jormanainen V., Parhiala K., Niemi A., Erhola M., Keskimäki I., Kaila M. (2019). Half of the Finnish Population Accessed Their Own Data: Comprehensive Access to Personal Health Information Online Is a Corner-Stone of Digital Revolution in Finnish Health and Social Care. Finn. J. eHealth Welf. 11 (4). 10.23996/fjhw.83323

80 Molnar-Gabor F., Sellner J., Pagil S., Slokenberga S., Tzortzatou O., Nyström K. (Forthcoming 2021). Harmonization after the GDPR? Divergences in the Rules for Genetic and Health Data Sharing in Four Member States and Ways to Overcome Them by EU Measures: Insights from Germany, Greece, Latvia and Sweden. Seminars in Cancer Biology.

81 Digital Health Laws and Regulations United Kingdom. ICLG. 2022

82 Guide to the UK General Data Protection Regulation (UK GDPR).

83 The Data Protection Act 2018, UK.

84 Ibid.

85 The UK General Data Protection Regulation (UK GDPR).

86 The Data Protection Act 2018, UK.

87 The Data Protection Act 2018, UK.

88 Policy paper. Data saves lives: reshaping health and social care with data. Department of Health & Social Care. 2022.

89 Policy paper. Data saves lives: reshaping health and social care with data. Department of Health & Social Care. 2022.

90 How do we ensure anonymisation is effective? Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. ICO. 2021.

91 How do we ensure anonymisation is effective? Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. ICO. 2021.

92 The Health Insurance Portability and Accountability Act of 1996 (HIPAA). // https://www.cdc.gov/phlp/publications/topic/hipaa.html

93 Health Insurance Portability and Accountability Act of 1996 (HIPAA).

94 The Health Information Technology for Economic and Clinical Health Act, 2009 (HITECH).

95 The Health Information Technology for Economic and Clinical Health Act, 2009 (HITECH).

96 The Genetic Information Nondiscrimination Act of 2008 (GINA).

97 Например, Иллинойс (Illinois Biometric Information Privacy Act, 2008), Вашингтон (Washington Biometric Information Privacy Act, 2017), Флорида (Florida Biometric Information Privacy Act, 2019).

98 Информационное письмо от 17.01.2018 по вопросам повторного использования медицинских данных; ИП от 17.01.2018 по вопросам сотрудничества, основанного на вторичном использовании медицинских данных; ИП от 11.11.2019 о доступе пациентов к персональным медицинским данным: «Здравоохранение под вашим контролем» (GD Circular, dated 17 January 2018, regarding secondary uses of health data. GD Circular, dated 17 January 2018, regarding collaborations based on secondary uses of health data. GD Circular, dated 11 November 2019, regarding patient access to personal health data: "Healthcare under your Control.").

99 Gesetz über die Spende, Entnahme und Übertragung von Organen und Gewebe. // https://www.gesetze-im-internet.de/tpg/TPG.pdf

100 Gesetz über die Spende, Entnahme und Übertragung von Organen und Gewebe

101 Digitales Versorgungsgesetz, 2019

102 Code de la santé publique // https://www.legifrance.gouv.fr

103 Code de la santé publique // https://www.legifrance.gouv.fr

104 Code de la santé publique // https://www.legifrance.gouv.fr

105 Code de la santé publique // https://www.legifrance.gouv.fr

106 ISO 9000:2015 - Quality management systems -- Fundamentals and vocabulary, URL http://www.iso.org/iso/catalogue_detail?csnumber=45481

107 N. Laranjeiro, et al, A Survey on Data Quality: Classifying Poor Data, IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC), 2015. P 179–188. EY, Big Data: changing the way businesses operate, см.: http://www.ey.com/Publication/vwLUAssets /EY-Big_data: changing_ the way businesses_ operate/ $FILE /EY-Insights-on-GRC-Big-data.pdf.

108 A. Immonen, P. Paakkonen, and E. Ovaska, Evaluating the Quality of Social Media Data in Big Data Architecture. IEEE Access, Volume 3, Pages: 2028–2043 October 16, 2015.

109 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

110 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

111 Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097), as last amended by Article 10 of the Act of 23 June 2021 (Federal Law Gazette I, p. 1858; 2022 I p. 1045).

112 Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 N 28608).

113 Independent report Unlocking the value of data: Exploring the role of data intermediaries. 2021. P. 16.

114 См. сайт организации Luna DNA https://www.lunadna.com

115 Park YT, Han D. Current Status of Electronic Medical Record Systems in Hospitals and Clinics in Korea. Healthc Inform Res. 2017 Jul;23(3):189-198. doi: 10.4258/hir.2017.23.3.189. Epub 2017 Jul 31. PMID: 28875054; PMCID: PMC5572523. P. 197.

116 Personal Information Protection Act (General Law) // https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=33

117 Bioethics And Safety Act. Act No. 16372, Apr. 23, 2019 // https://elaw.klri.re.kr/kor_service/lawView.do?lang=ENG&hseq=52559

118 Bioethics And Safety Act. Act No. 16372, Apr. 23, 2019 // https://elaw.klri.re.kr/kor_service/lawView.do?lang=ENG&hseq=52559

119 Bioethics And Safety Act. Act No. 16372, Apr. 23, 2019 // https://elaw.klri.re.kr/kor_service/lawView.do?lang=ENG&hseq=52559

120 Bioethics And Safety Act. Act No. 16372, Apr. 23, 2019 // https://elaw.klri.re.kr/kor_service/lawView.do?lang=ENG&hseq=52559

121 KDIS Working Paper 20-19, Regulatory Reform for Fostering an Innovation, Ecosystem, Sooyoung Oh, Changyong Choi, Ju-Ho Lee. P. 28.

122 Chang, JH, H Moon, J Oh, JH Kim, CI Kim, and J Yang. 2020. Regulatory Reform in Korea Interview by Sooyoung O. P. 1–4.

123 Framework Act on Administrative Regulations (Enforced on 2019.7.17); Enforcement Decree of the Special Act on Promotion of Information and Communications Technology, Vitalization of Convergence Thereof, etc. (Enforced on 2019.1.17); Industrial Convergence Promotion Act (Enforced on 2019.1.17); Act on Special Cases Concerning the Regulation of Regulation-Free Special Zones and Special Economic Zones for Specialized Regional Development (Enforced on 2019.1.17); Special Act on Support for Financial Innovation (Enforced on 2019.4.1); Act on the Promotion of Smart City Development and Industry (Enforced on 2020.2.27)

124 Положение о «Пересмотре некоторых положений о средствах генетического тестирования, которые могут проводиться непосредственно учреждениями генетического тестирования» см. http://www.mohw.go.kr/react/jb/sjb0406vw.jsp?PAR_MENU_ID=03&MENU_ID=030406&page=1&CONT_SEQ=352888

125 См. Lee GY, Han SN. Direct-to-Consumer Genetic Testing in Korea: Current Status and Significance in Clinical Nutrition. Clin Nutr Res. 2021 Oct;10(4). https://doi.org/10.7762/cnr.2021.10.4.279 P. 279–291. Regulatory Sandbox: Health RegLab Design Elements. // https://www.uaepublicpolicyforum.ae/wp-content/uploads/2020/02/Sandboxing.pdf P. 18

126 Ministry of Health and Welfare. Partial revision of regulations on genetic testing items that can be directly conducted by genetic testing institutions other than medical institutions. 2020 //http://www.mohw.go.kr/react/jb/sjb0406vw.jsp?PAR_MENU_ID=03&MENU_ID=030406&page=1&CONT_SEQ=352888.

127 Biotechnology leader Macrogen advances DNA-tailored health care in Asia. The company is using its R&D and technological expertise in genomics to create solutions based on big data for individual benefit. // https://www.scmp.com/country-reports/country-reports/topics/south-korea-business-report-2020/article/3079838?module=perpetual_scroll_0&pgtype=article&campaign=3079838

128 Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

129 Biotechnology leader Macrogen advances DNA-tailored health care in Asia. The company is using its R&D and technological expertise in genomics to create solutions based on big data for individual benefit. // https://www.scmp.com/country-reports/country-reports/topics/south-korea-business-report-2020/article/3079838?module=perpetual_scroll_0&pgtype=article&campaign=3079838

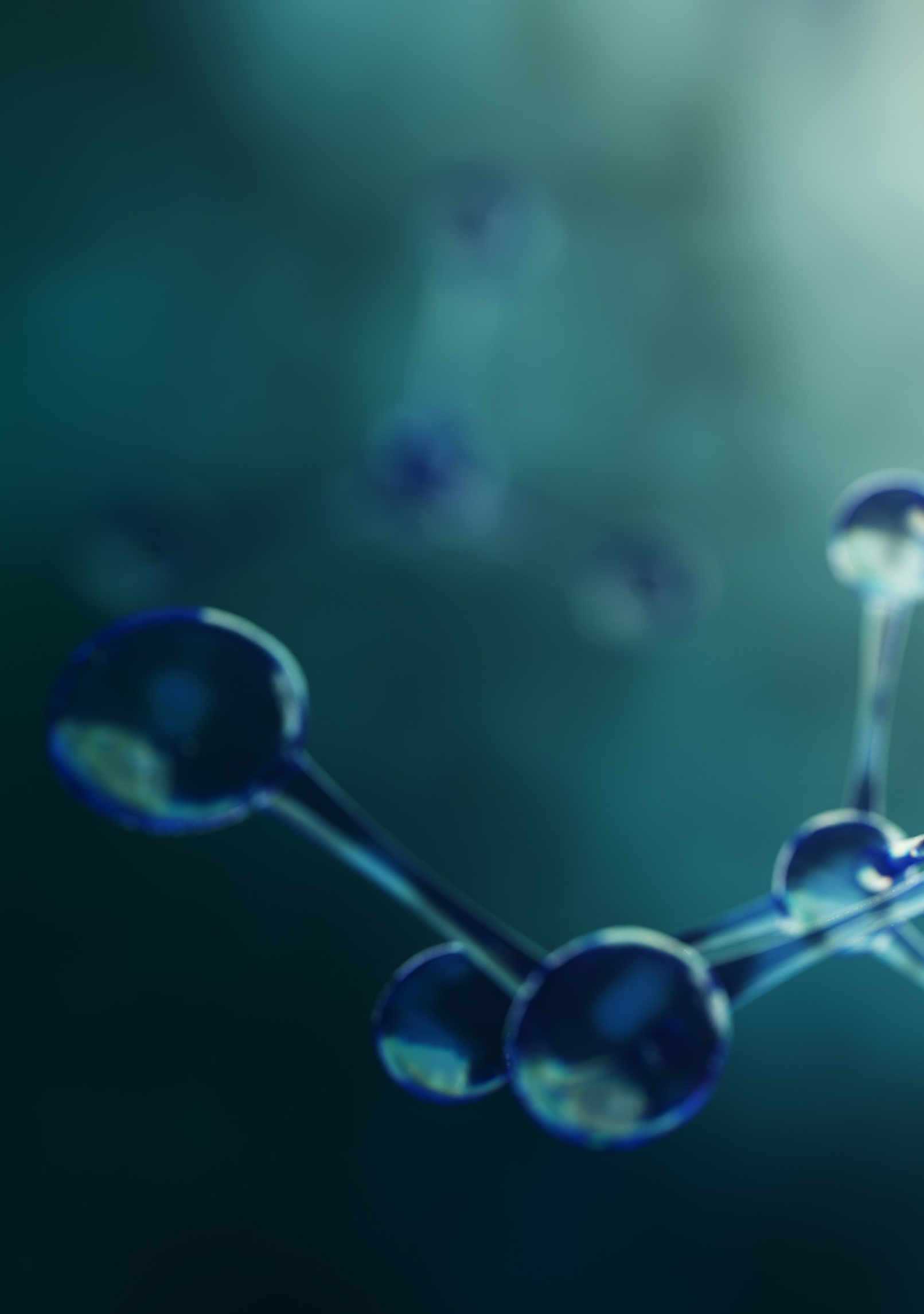
130 https://www.korea.net/NewsFocus/Sci-Tech/view?articleId=168047

131 Personal Information Protection Act (General Law) // https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=33

132 The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users. 2020. https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.pdf;jsessionid=BA64ACB035CF64CE4296925C54B39228.1_cid354?__blob=publicationFile&v=2

133 Sozialgesetzbuch (SGB V) Fünftes Buch Gesetzliche Krankenversicherung Stand: Zuletzt geändert durch Art. 2 G v. 16.9.2022 I 1454 § 139e SGB V Verzeichnis für digitale Gesundheitsanwendungen; Verordnungsermächtigung // https://www.sozialgesetzbuch-sgb.de/sgbv/139e.html

134 The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users. 2020. https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.pdf;jsessionid=BA64ACB035CF64CE4296925C54B39228.1_cid354?__blob=publicationFile&v=2

Электронная версия доклада

Сайт АНО «Цифровая экономика»
data-economy.ru