

Ф.У. Юсупова*

PhD, доцент, Институт переподготовки и повышения
квалификации юридических кадров при
Министерстве юстиции Республики Узбекистан, Ташкент, Узбекистан
*Автор для корреспонденции: Faringiz002@gmail.com

ПРАВОВЫЕ ГАРАНТИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ МЕДИЦИНСКИХ УСЛУГ: ЗАРУБЕЖНЫЙ ОПЫТ

Аннотация

В статье рассматриваются правовые гарантии защиты персональных данных пациента в условиях цифровизации медицинских услуг на основе анализа зарубежного опыта. Особое внимание уделяется трансформации традиционного института врачебной тайны в условиях внедрения электронных медицинских карт, цифровых платформ, телемедицинских сервисов и автоматизированных информационных систем здравоохранения. Обосновывается, что персональные данные пациента, включая сведения о состоянии здоровья, диагнозе, результатах обследования и лечении, относятся к особо чувствительной категории информации и требуют усиленной правовой, организационной и технической защиты. На основе зарубежного опыта раскрываются такие гарантии, как получение согласия пациента на обработку медицинских данных, целевой характер их использования, обеспечение конфиденциальности, информационной безопасности, контроль доступа к электронным базам данных, а также право пациента на получение информации об обработке его персональных данных. В статье подчеркивается необходимость перехода от формального запрета разглашения врачебной тайны к комплексной модели защиты персональных медицинских данных, включающей правовые, договорные, технические и организационные механизмы. Вывод - значимость зарубежного опыта для совершенствования национального законодательства в сфере цифрового здравоохранения и усиления гарантий защиты прав пациента.

Ключевые слова: персональные данные пациента, медицинские данные, врачебная тайна, цифровизация медицинских услуг, цифровое здравоохранение.

Введение

В современных условиях цифровизация медицинских услуг становится одним из ключевых направлений развития системы здравоохранения. Внедрение электронных медицинских карт, цифровых платформ, телемедицинских сервисов, автоматизированных информационных систем и облачных технологий способствует повышению качества, доступности и оперативности медицинской помощи. Вместе с тем активное использование цифровых технологий в сфере здравоохранения существенно увеличивает объем обрабатываемых персональных данных пациента и порождает новые правовые риски, связанные с их незаконным сбором, хранением, передачей, использованием и раскрытием.

Особую значимость в данном контексте приобретают персональные данные пациента, поскольку сведения о состоянии здоровья, диагнозе, результатах обследований, назначенном лечении, наследственных особенностях и иных медицинских обстоятельствах относятся к наиболее чувствительной категории информации. Незаконное распространение либо неправомерная обработка таких данных может повлечь нарушение права на неприкосновенность частной жизни, причинение морального вреда, дискриминацию, репутационные потери, а также снижение доверия граждан к системе здравоохранения. Поэтому защита персональных данных пациента должна рассматриваться не только как обязанность медицинской организации или медицинского работника, но и как важная правовая гарантия реализации конституционных прав личности.

Институт врачебной тайны в условиях цифровизации медицинских услуг уже не может рассматриваться как единственный и достаточный механизм защиты медицинской

информации. Если ранее основная угроза была связана преимущественно с разглашением сведений медицинским работником, то в настоящее время риски охватывают также несанкционированный доступ к электронным базам данных, передачу информации третьим лицам, интеграцию медицинских информационных систем, недостаточную техническую защищенность цифровых платформ, а также обработку данных без надлежащего согласия пациента.

В этом отношении особый научный и практический интерес представляет сравнительно-правовой анализ опыта Узбекистана и Казахстана. Оба государства осуществляют реформирование системы здравоохранения, внедряют цифровые технологии в медицинскую сферу и развивают правовые механизмы защиты персональных данных. Вместе с тем подходы к регулированию медицинской тайны, согласия пациента, обработки электронных медицинских данных и обеспечения информационной безопасности имеют определенные особенности, выявление которых позволяет определить направления дальнейшего совершенствования национального законодательства.

Методы

В Республике Узбекистан развитие цифрового здравоохранения и расширение договорных отношений при оказании медицинских услуг требуют более четкого закрепления правовых гарантий защиты персональных данных пациента. Особое значение имеют вопросы включения в договоры оказания медицинских услуг специальных условий о сборе, хранении, обработке, передаче и защите медицинских данных, а также об ответственности за нарушение конфиденциальности. При этом действующая практика нередко ограничивается общим указанием на обязанность сохранения врачебной тайны, что не всегда соответствует современным требованиям цифровой медицины.

Опыт Республики Казахстан представляет интерес с точки зрения нормативного закрепления специальных гарантий защиты медицинских данных в цифровой среде. В казахстанском законодательстве уделяется внимание вопросам согласия пациента, ограничения использования персонифицированных данных, а также недопущения подключения автоматизированных баз данных, содержащих сведения о частной жизни пациента, к иным информационным системам без его согласия. Такой подход свидетельствует о признании согласия пациента центральным элементом правового режима обработки медицинских данных.

Договор оказания медицинских услуг в современной системе здравоохранения выступает не только средством закрепления гражданско-правовых обязательств, но и важным правовым механизмом защиты данных пациента. В рамках данного договора правоотношения, возникающие между медицинской организацией и пациентом, охватывают не только качество и объем оказываемых медицинских услуг, но и обязанность по обеспечению конфиденциальности персональных и медицинских данных пациента. Особенно в условиях развития цифровой медицины и электронных систем здравоохранения возрастает риск незаконного раскрытия сведений о пациенте, их передачи третьим лицам либо ненадлежащей обработки. С этой точки зрения договор оказания медицинских услуг приобретает особое значение как правовая гарантия, направленная на предупреждение указанных рисков.

Первоначально в соответствии с Указом Президента Республики Узбекистан от 26 февраля 2003 года № УП–3214 «О мерах по дальнейшему реформированию системы здравоохранения» на базе ведущих медицинских клиник республики в экспериментальном порядке были созданы четыре Республиканских специализированных медицинских центра по урологии, хирургии, микрохирургии глаза и кардиологии. Данные центры были призваны оказывать населению высококвалифицированную медицинскую помощь с использованием современных высокотехнологичных диагностических и лечебных медицинских средств[1].

Были определены порядок и тарифы оказания населению высококвалифицированной медицинской помощи на платной основе, условия бесплатного лечения льготных категорий пациентов, а также порядок поэтапного перехода центров на принципы самофинансирования и самоокупаемости.

В соответствии с постановлением Кабинета Министров Республики Узбекистан от 8 июня 2004 года № 264 «О мерах по завершению эксперимента и углублению реформ в системе здравоохранения» проводимые в системе здравоохранения Республики Узбекистан реформы направлены также на усиление обязательности договорных отношений при оказании медицинских услуг. В практической деятельности особо подчеркивается необходимость заключения договора между медицинским учреждением и пациентом [2].

Это позволяет рассматривать договор не только как экономико-правовой документ, но и как средство обеспечения неприкосновенности частной жизни пациента. В таком договоре должны быть четко определены порядок сбора, хранения, обработки и передачи данных пациента, а также законные основания их раскрытия. Тем самым договор служит обеспечению сохранения врачебной тайны, защите персональных данных и реализации принципа согласия пациента.

Согласно научным подходам, договор оказания медицинских услуг выражает систему двусторонних обязательств. С одной стороны, медицинская организация принимает на себя обязанность оказывать пациенту качественную медицинскую помощь и одновременно сохранять конфиденциальность его данных. С другой стороны, пациент, предоставляя свои данные, пользуется медицинскими услугами, однако сохраняет право требовать, чтобы эти данные использовались исключительно в установленных целях. В этом аспекте договор может рассматриваться как средство практического обеспечения права пациента на информационное самоопределение [3].

Договор оказания медицинских услуг в современной правовой системе является комплексным инструментом защиты данных пациента, посредством которого взаимно согласуются институт врачебной тайны, нормы о защите персональных данных и принцип согласия пациента. В связи с этим совершенствование содержания данного договора в национальном законодательстве, особенно путем закрепления в нем четких и обязательных положений о защите данных, является актуальной задачей [4].

Правовая природа медицинской тайны, врачебной тайны и персональных данных, их соотношение, а также зарубежный опыт в сравнении с национальным законодательством. В результате проведенного анализа установлено, что в современных правовых системах медицинские данные признаются особой категорией информации, подлежащей повышенному уровню защиты.

Результаты и обсуждения

Так, известный ученый-правовед А. Вестин трактует защиту персональных данных как право индивида осуществлять контроль над информацией о своей личности. Данный подход в полной мере применим и к медицинским данным, поскольку он обосновывает необходимость обеспечения права пациента контролировать сведения, касающиеся состояния его здоровья [5].

Представитель европейской правовой школы Л. Бюгрейв отмечает, что данные, связанные со здоровьем, относятся к специальной категории персональных данных и требуют применения усиленных правовых и технических мер защиты по сравнению с обычными персональными данными. Данные идеи нашли отражение и в Общем регламенте Европейского союза о защите данных — GDPR, где установлены строгие условия обработки медицинских данных [6].

Кроме того, американский исследователь Д. Солов подчеркивает, что проблему защиты персональных данных нельзя сводить только к конфиденциальности. Она требует комплексного подхода, включающего контроль над данными, предупреждение их неправомерного использования и обеспечение информационной безопасности. Эта концепция особенно актуальна в условиях цифровой медицины и широко применяется в сфере обращения электронных медицинских данных [7].

В научных взглядах российских ученых М.М. Малеиной и О.С. Иоффе врачебная тайна также рассматривается как важный элемент неприкосновенности частной жизни граждан. При этом подчеркивается, что ее раскрытие возможно только в исключительных случаях, прямо

предусмотренных законом. По их мнению, договорные механизмы имеют особое значение при работе с медицинскими данными, поскольку именно посредством договора четко определяются права и обязанности сторон[8].

Исходя из приведенных научных подходов, при заключении договоров оказания медицинских услуг необходимо комплексно отражать положения, касающиеся медицинской тайны, врачебной тайны и защиты персональных данных. В действующей договорной практике, однако, нередко наблюдается ограничение только обязанностью не разглашать «врачебную тайну», что не в полной мере соответствует требованиям современной цифровой системы здравоохранения.

В современных условиях, когда широко внедряются платформы DMED, электронные медицинские карты EHR/EMR, телемедицина и облачные технологии, договор оказания медицинских услуг должен охватывать также вопросы безопасности электронных данных. В этом отношении П. Фойгт и А. фон дем Буше в комментариях к GDPR выдвигают принципы “privacy by design” и “privacy by default” как современную модель защиты данных. Эти принципы должны применяться и к договорам оказания медицинских услуг, что означает необходимость заранее закреплять меры по защите данных на договорном уровне[9].

В связи с этим можно научно обосновать, что договор оказания медицинских услуг должен включать не только традиционные обязательства по соблюдению конфиденциальности, но и конкретные требования, направленные на обеспечение безопасности электронных медицинских данных. Это превращает договор в комплексный и эффективный правовой механизм защиты данных пациента и способствует приближению национального законодательства к международным стандартам.

Зарубежный опыт, в частности GDPR Европейского союза и законодательство США HIPAA, показывает, что защита медицинских данных должна охватывать не только конфиденциальность, но и безопасность данных, прозрачность их обработки, а также обеспечение права субъекта данных на контроль. В этом контексте особое значение имеет научный подход Д. Солова, который рассматривает конфиденциальность в широком смысле — как комплексный институт, неразрывно связанный с контролем над информацией и ее безопасностью.

В зарубежной практике в договорах оказания медицинских услуг положения о защите данных пациента часто включаются в качестве самостоятельного раздела. Так, в практике США в соответствии с требованиями HIPAA субъекты, оказывающие медицинские услуги, закрепляют в договорах конкретные обязанности по защите электронных медицинских данных пациента. В Европейском союзе на основе принципов “privacy by design” и “privacy by default” меры по защите данных должны быть интегрированы в договор и информационную систему уже на начальном этапе[10].

В США защита медицинских данных развивалась на основе законодательства HIPAA, в котором договорные механизмы занимают особое место. В частности, в договорах оказания медицинских услуг четко определяется порядок использования, обработки и защиты сведений о состоянии здоровья пациента — Protected Health Information, PHI. В соответствии с HIPAA Privacy Rule такие данные могут использоваться только для целей лечения, оплаты и осуществления деятельности в сфере здравоохранения. Security Rule, в свою очередь, устанавливает обязательные технические и организационные меры по защите электронных медицинских данных — e-PHI [11].

Кроме того, в практике США широко применяется институт Business Associate Agreement, предусматривающий обязательные договорные отношения с третьими лицами, работающими с медицинскими данными. В таких договорах четко регулируются пределы использования данных, обязанности по соблюдению требований информационной безопасности, обязательство уведомления при нарушении безопасности данных, а также вопросы ответственности.

Данный подход показывает, что в США защита медицинских данных обеспечивается не только на уровне законодательства, но и посредством договорных механизмов. Поэтому в

национальной практике также целесообразно включать в договоры оказания медицинских услуг конкретные положения, касающиеся обеспечения безопасности электронных медицинских данных.

В условиях стремительного развития цифровых технологий и обработки большей части медицинских данных в электронной форме эффективная правовая защита персональных данных становится необходимым условием сохранения доверия граждан к системе здравоохранения и предупреждения возможных злоупотреблений. Нормы, направленные на обеспечение защиты таких данных, регулируют процессы сбора, хранения, обработки и передачи информации, предупреждают дискриминацию и гарантируют соблюдение прав пациента в цифровой среде.

В Республике Казахстан, являющейся одним из государств СНГ, вопросы обеспечения безопасности медицинских данных достаточно четко урегулированы на нормативно-правовом уровне. В частности, в Кодексе Республики Казахстан «О здоровье народа и системе здравоохранения» закреплены специальные гарантии, согласно которым не допускается внесение в автоматизированные базы данных персонифицированных сведений, касающихся частной жизни пациента, а также их использование без его согласия.

Кроме того, в соответствии с нормами указанного кодекса при использовании сведений, относящихся к частной жизни, запрещается без согласия пациента подключать автоматизированные базы данных, содержащие персонифицированные сведения, к сетям, интегрирующим их с иными информационными системами.

Данный подход свидетельствует о центральной роли согласия пациента в отношениях, связанных с медицинскими данными, и выступает важным правовым механизмом обеспечения защиты персональных данных в цифровой среде.

С учетом научно-технического прогресса, развития телемедицины, внедрения компьютерной обработки медицинских данных и появления новых информационных систем позиция законодателя по данному вопросу представляется всесторонне обоснованной. Быстрое развитие инновационных технологий, распространение интернета и дистанционных услуг требуют новых правил обеспечения конфиденциальности информации, защиты данных от неправомерного доступа и раскрытия.

В связи с этим вопросы информационной безопасности и ее правового обеспечения постоянно находятся в центре внимания государства. Ведется активная работа по обновлению требований, предъявляемых к медицинским информационным системам. Защита медицинских данных, в том числе сведений, составляющих врачебную тайну, обеспечивается путем установления дополнительных норм, обязательных для всех субъектов здравоохранения независимо от формы собственности. Эти нормы касаются контроля доступа, защиты персональных данных, предупреждения технических сбоев, индивидуального учета пользователей и мониторинга их активности.

Анализ развития института медицинской тайны показывает, что представления исполнителей медицинских услуг о ее морально-этическом содержании и допустимости раскрытия в разные исторические периоды менялись: от полного отрицания возможности существования конфиденциальных сведений о здоровье пациента до убеждения в необходимости абсолютного сохранения всех сведений, относящихся к медицинскому учету личности. В настоящее время правовой подход к данной проблеме отличается большей определенностью. Признание информации, в том числе врачебной тайны, объектом гражданских прав позволило законодателю определить формы ее выражения, а также урегулировать порядок ее сбора, хранения и распространения.

Исходя из указанных зарубежных подходов, возникает необходимость совершенствования договоров оказания медицинских услуг, применяемых в национальной практике. В действующих договорах, как правило, предусматривается лишь обязанность не разглашать «врачебную тайну», тогда как современные риски, связанные с обращением электронных медицинских данных, учитываются недостаточно. Между тем сегодня данные

пациента широко обрабатываются через платформы DMED, электронные медицинские карты EHR/EMR и системы телемедицины.

В случае нарушения законных прав пациента он вправе требовать компенсации причиненного ему морального вреда. Следует отметить, что пациент может воспользоваться данным способом защиты только в том случае, если лицо, оказывающее медицинские услуги, виновно нарушило его права. Это положение закреплено в статье 1021 Гражданского кодекса Республики Узбекистан, а также в статье 22 Закона «О защите прав потребителей»[12].

Вместе с тем представляется более справедливым установить возможность компенсации морального вреда за разглашение тайны, касающейся пациента, независимо от вины причинителя вреда. Такое решение законодателя соответствовало бы принципу гуманизма по отношению к потерпевшему. Подобная возможность уже предусмотрена гражданским законодательством, в частности статьей 1021 Гражданского кодекса Республики Узбекистан, где определены основания компенсации вреда независимо от вины. Среди них указаны случаи причинения вреда жизни и здоровью гражданина источником повышенной опасности, а также причинения вреда путем распространения сведений, порочащих честь, достоинство и деловую репутацию лица.

На наш взгляд, предоставление такой льготы потерпевшей стороне объясняется стремлением законодателя защитить наиболее значимые для гражданина нематериальные блага и права, а также обеспечить их эффективную охрану.

Раскрытие сведений, составляющих профессиональную тайну медицинского работника, несомненно, влечет для потерпевшего психоэмоциональные последствия. К ним относятся переживания, тревожность, чувство уязвимости, ощущение неполноценности в глазах общества и состояние безысходности. Внесение в законодательство изменений, предусматривающих возможность компенсации морального вреда независимо от вины, будет стимулировать медицинских работников к добросовестному исполнению своих обязанностей, укрепит защиту права гражданина на личную неприкосновенность и установит строгие границы от несанкционированного вмешательства в частную жизнь.

Если раскрытие тайны произошло через средства массовой информации, защита нарушенного права должна осуществляться в рамках иска о защите чести, достоинства и деловой репутации.

Поэтому, опираясь на зарубежный опыт, целесообразно включать в договоры оказания медицинских услуг четкие и обязательные условия, направленные на обеспечение безопасности электронных медицинских данных. В условиях цифровой системы здравоохранения договор выступает не только правовой основой оказания услуг, но и важной гарантией защиты персональных данных пациента.

Характеризуя элементы договора оказания медицинских услуг, следует отметить, что одним из важных условий, обеспечивающих определенность правоотношений между исполнителем и пациентом, а также эффективную защиту прав пациента, является четкое закрепление сроков в договоре.

Специфика медицинских услуг заключается в том, что ожидаемый от них результат не всегда может быть точно спрогнозирован во времени. Вместе с тем сложность процесса лечения, индивидуальное физиологическое состояние пациента, стадия заболевания и внешние факторы непосредственно влияют на сроки оказания медицинских услуг. С учетом данных обстоятельств исполнитель должен определить разумный срок для каждого пациента.

В действующем законодательстве в сфере здравоохранения отсутствуют нормы, прямо регулирующие сроки оказания медицинской помощи, за исключением специальных требований, касающихся сроков оказания скорой медицинской помощи. Если заболевание или состояние угрожает жизни гражданина либо такая угроза должна быть устранена на месте происшествия и/или по пути в медицинскую организацию, скорая медицинская помощь должна быть оказана в экстренном и неотложном порядке.

При отсутствии соглашения между сторонами о сроках оказания медицинских услуг данный срок определяется путем толкования договора в соответствии с пунктом 2 статьи 145

Гражданского кодекса Республики Узбекистан. При этом учитываются особенности медицинской деятельности, обстоятельства, послужившие основанием для обращения пациента за медицинской помощью, ожидаемые результаты, объем медицинских процедур, способы их проведения, необходимость предварительной подготовки пациента и иные обстоятельства[13].

Характеризуя элементы договора оказания медицинских услуг, необходимо обратить внимание на то, что срок должен быть согласован в договоре как важное условие, обеспечивающее определенность правоотношений и реализацию прав пациента. С учетом специфики медицинских услуг, невозможности во всех случаях точно прогнозировать ожидаемый эффект во времени, а также рисков, способных повлиять на своевременность их оказания, исполнитель должен определить разумный срок применительно к состоянию здоровья конкретного пациента. При этом должны учитываться характер необходимых лечебно-диагностических процедур, содержание медицинских стандартов, внешние обстоятельства, сопутствующие оказанию медицинской услуги, а также уровень современных достижений медицинской науки. Разумный срок может включать период подготовки пациента к медицинскому вмешательству и период восстановления после него.

Согласованный в договоре разумный срок должен обеспечивать исполнителю возможность оказания качественной услуги, соответствовать критериям объективности с учетом обстоятельств конкретного пациента и быть ориентированным на деятельность надлежащей медицинской организации, располагающей необходимыми ресурсами и специалистами. Особое юридическое значение имеют случаи, когда пациент не исполняет свои обязанности и тем самым лишает исполнителя возможности провести либо завершить медицинское вмешательство в согласованный срок. Такие обстоятельства следует рассматривать как просрочку кредитора.

По нашему мнению, срок в рассматриваемом договоре должен быть отражен как самостоятельная категория, по крайней мере путем установления срока начала оказания медицинских услуг. Современные достижения медицины, техническая оснащенность медицинской деятельности, а также практический опыт и квалификация исполнителей позволяют достаточно точно прогнозировать соответствующие сроки. Если медицинские услуги носят комплексный характер либо оказываются несколькими исполнителями, согласование сроков приобретает особенно важное значение.

Особый интерес для сравнительно-правового анализа представляет опыт Республики Казахстан, поскольку в данной стране вопросы защиты персональных медицинских данных в условиях цифровизации здравоохранения получили более детальное нормативное закрепление. В отличие от традиционного подхода, при котором медицинская информация охраняется преимущественно через институт врачебной тайны, казахстанское законодательство формирует комплексную модель регулирования, охватывающую сбор, обработку, хранение, защиту и предоставление персональных медицинских данных в цифровой среде [14].

В Республике Казахстан правовой режим медицинской информации определяется не только общими нормами о персональных данных, но и специальными положениями законодательства о цифровом здравоохранении. В частности, в Правилах осуществления сбора, обработки, хранения, защиты и предоставления персональных медицинских данных субъектами цифрового здравоохранения персональные медицинские данные определяются как персональные данные, содержащие сведения о здоровье физического лица и оказанных ему медицинских услугах, зафиксированные на электронных, бумажных или иных материальных носителях [15]. Такой подход позволяет охватывать правовой защитой как традиционные медицинские документы, так и электронные медицинские записи, формируемые в медицинских информационных системах.

Кроме того, в казахстанском законодательстве закрепляется понятие тайны медицинского работника, к которой относятся персональные медицинские данные, информация о факте обращения за медицинской помощью, состоянии здоровья лица, диагнозе

его заболевания и иные сведения, полученные при обследовании и лечении пациента [16]. Это свидетельствует о том, что медицинские данные рассматриваются как особая категория информации, требующая повышенного уровня правовой, организационной и технической защиты.

Значимым элементом казахстанской модели является специальное регулирование согласия пациента на обработку персональных медицинских данных. Пациент или его законный представитель дает согласие на сбор и обработку таких данных в письменной форме, в форме электронного документа либо через кабинет пользователя на веб-портале «электронного правительства» [17]. Данный механизм имеет важное значение, поскольку он адаптирует институт согласия пациента к условиям цифровой медицины и обеспечивает возможность его реализации не только в бумажной, но и в электронной форме.

Казахстанское законодательство также устанавливает целевой характер обработки персональных медицинских данных. Так, обработка персональных медицинских данных пациентов субъектами цифрового здравоохранения осуществляется исключительно для оказания медицинской помощи. Одновременно предусматривается обязанность субъектов цифрового здравоохранения обеспечивать конфиденциальность, целостность и доступность персональных медицинских данных посредством организационных и технических мер защиты информации [18].

Особое значение имеет то, что в Казахстане урегулированы вопросы хранения и технической защиты электронных медицинских данных. В частности, персональные медицинские данные подлежат хранению на серверах, физически размещенных на территории Республики Казахстан. Кроме того, субъекты цифрового здравоохранения обязаны осуществлять контроль доступа к информационным системам путем протоколирования и журналирования действий пользователей, а также обеспечивать резервное копирование медицинской документации в электронной форме [19]. Указанные меры свидетельствуют о стремлении законодателя обеспечить не только конфиденциальность, но и информационную безопасность медицинских данных.

Важной особенностью казахстанского подхода является закрепление права пациента на получение информации о своих персональных медицинских данных. Пациент или его законный представитель вправе обратиться к субъекту цифрового здравоохранения с запросом и получить сведения о наличии персональных медицинских данных, целях, источниках и способах их сбора и обработки, перечне обрабатываемых данных, а также сроках их обработки и хранения [20]. Такой механизм усиливает контроль пациента над своими медицинскими данными и способствует реализации принципа информационного самоопределения.

Сравнивая данный подход с законодательством Республики Узбекистан, следует отметить, что в Узбекистане правовая охрана медицинской информации традиционно строится на институте врачебной тайны. В соответствии с Законом Республики Узбекистан «Об охране здоровья граждан» информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при обследовании и лечении, составляют врачебную тайну. Не допускается разглашение таких сведений без согласия гражданина или его законного представителя, за исключением случаев, прямо предусмотренных законом.

Кроме того, узбекское законодательство закрепляет право пациента на сохранение в тайне информации о факте обращения за медицинской помощью, состоянии здоровья, диагнозе и иных сведениях, полученных при обследовании и лечении. Информация, содержащаяся в медицинских документах гражданина, также признается врачебной тайной и может предоставляться без его согласия только по основаниям, предусмотренным законом. Следовательно, законодательство Узбекистана обеспечивает базовую правовую защиту медицинской информации пациента через институт врачебной тайны и согласия пациента.

Наряду с этим Закон Республики Узбекистан «О персональных данных» устанавливает общие требования к сбору, хранению, использованию, распространению и защите персональных данных. В частности, использование персональных данных допускается только

для ранее заявленных целей их сбора при обеспечении необходимого уровня защищенности, а лица, получившие доступ к персональным данным, обязаны не допускать их разглашения. Эти положения имеют значение и для сферы здравоохранения, поскольку медицинские данные пациента одновременно являются персональными данными.

Вместе с тем сравнительный анализ показывает, что казахстанская модель более детально адаптирована к условиям цифровизации медицинских услуг. Если в Узбекистане основной акцент сделан на запрете разглашения врачебной тайны и общих положениях о защите персональных данных, то в Казахстане дополнительно урегулированы специальные вопросы цифрового оборота персональных медицинских данных: их сбор, обработка, хранение, предоставление, обезличивание, техническая защита, электронное согласие пациента, право пациента получать сведения о своих данных, а также контроль действий пользователей в медицинских информационных системах.

Заключение

Таким образом, общее сходство правового регулирования Узбекистана и Казахстана заключается в признании медицинской информации конфиденциальной и недопустимости ее разглашения без согласия пациента, за исключением предусмотренных законом случаев. В обоих государствах медицинские данные рассматриваются как информация, непосредственно связанная с частной жизнью лица, его здоровьем и личной неприкосновенностью. Поэтому их защита имеет не только отраслевое, но и конституционно-правовое значение.

В то же время различие состоит в степени детализации правового регулирования. В Республике Казахстан более четко закреплены специальные правила, ориентированные именно на цифровое здравоохранение и электронные медицинские данные. В Республике Узбекистан регулирование пока в большей степени основывается на общих положениях о врачебной тайне, персональных данных и правах пациента. В связи с этим представляется целесообразным использовать отдельные элементы казахстанского опыта при совершенствовании национального законодательства Узбекистана.

В частности, для Узбекистана представляет интерес закрепление специальных правил сбора, обработки, хранения, защиты и предоставления персональных медицинских данных в цифровой системе здравоохранения. Кроме того, целесообразно нормативно определить понятие «персональные медицинские данные», установить требования к электронному согласию пациента, закрепить обязанность медицинских организаций обеспечивать техническую защиту электронных медицинских записей, а также предусмотреть право пациента получать информацию о целях, способах, сроках и субъектах обработки его медицинских данных.

Следовательно, опыт Казахстана показывает, что защита персональных данных пациента в условиях цифровизации медицинских услуг должна выходить за рамки традиционного института врачебной тайны. Она должна включать комплекс правовых, организационных, технических и договорных гарантий, направленных на предупреждение незаконного доступа к медицинским данным, обеспечение прозрачности их обработки и усиление контроля пациента над информацией о своем здоровье. Для Республики Узбекистан данный подход может служить ориентиром при дальнейшем развитии законодательства о цифровом здравоохранении и защите персональных данных пациента.

Список литературы

1. О мерах по дальнейшему реформированию системы здравоохранения Указ Президента Республики Узбекистан, от 26.02.2003 г. № УП-3214, Доступно на: <https://lex.uz/uz/docs/-170143>
2. О мерах по завершению эксперимента и углублению реформ в системе здравоохранения Постановление Кабинета Министров Республики Узбекистан, от 08.06.2004 г. № 264 Доступно на: <https://lex.uz/uz/docs/-302557>
3. Westin A. Privacy and Freedom. — New York: Atheneum Доступно на <https://scholarlycommons.law.wlu.edu/wluhr/vol25/iss1/20/>

4. Bygrave L.A. Data Privacy Law: An International Perspective. — Oxford University Press, 2014. Доступно на: <https://dokumen.pub/data-privacy-law-an-international-perspective-9780199675555.html>
5. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008 Доступно на: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888
6. Крысанова Н. В. 2001. 04. 39. Малеина М. Н. Личные неимущественные права граждан: понятие, осуществление, защита. М. : МЗ Пресс, 2000. 244 с. Библиогр. : С. 237-242 // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Серия 4. Государство и право. 2001. №4. Доступно на: <https://cyberleninka.ru/article/n/2001-04-39-maleina-m-n-lichnye-neimuschestvennye-prava-grazhdan-ponyatie-osuschestvlenie-zaschita-m-mz-press-2000-244-s-bibliogr-s-237-242>
7. Voigt, P. and Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. 1st Edition, Springer International Publishing, Cham 2017, Доступно на: <https://doi.org/10.1007/978-3-319-57959-7>
8. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008 Доступно на: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888
9. Nozimakhon, G., & Faringiz, Y. Analysis of International Legislation Regulating the Protection of Patients' Rights. 2022, 5, 5–8. Доступно на: <https://doi.org/10.31557/APJEC.2022.5.S1.5>.
10. Кодекс Республики Казахстан от 7 июля 2020 года № 360-VI «О здоровье народа и системе здравоохранения» // ИПС НПА РК. Доступно на: <https://adilet.zan.kz/rus/docs/K2000000360> (Дата обращения: 07.09.2025)
11. Об утверждении правил осуществления сбора, обработки, хранения, защиты и предоставления персональных медицинских данных субъектами цифрового здравоохранения Приказ Министра здравоохранения Республики Казахстан от 14 апреля 2021 года № КР ДСМ -30. Зарегистрирован в Министерстве юстиции Республики Казахстан 15 апреля 2021 года № 22550. Доступно на: <https://adilet.zan.kz/rus/docs/V2100022550/compare>
12. Гражданский кодекс Республики Узбекистан, Доступно на: <https://lex.uz/docs/-180552>
13. Юсупова, Ф. "Медицинские услуги в эпоху цифровой трансформации: правовые аспекты телемедицины." *LEGALITAS* 4.4 (2025): 74-81.
14. Об охране здоровья граждан Закон Республики Узбекистан, от 29.08.1996 г. № 265-I Доступно на <https://lex.uz/mact/-26013>
15. Гражданский кодекс Республики Узбекистан, Доступно на: <https://lex.uz/docs/-180552>
16. SC, I.F. (2013). Privacy and Confidentiality: The Doctor's Obligations. In: Beran, R. (eds) *Legal and Forensic Medicine*. Springer, Berlin, Heidelberg, Доступно на: https://doi.org/10.1007/978-3-642-32338-6_147
17. Кодекс Республики Казахстан от 7 июля 2020 года № 360-VI «О здоровье народа и системе здравоохранения» // ИПС НПА РК. – <https://adilet.zan.kz/rus/docs/K2000000360> (Дата обращения: 07.09.2025)
18. Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021. Licence: CC BY-NC-SA 3.0 IGO. Доступно на: <https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf>
19. Qizi YFU. Telemedicine in the Digital Era: Navigating the International Legal Landscape to Expand Global Healthcare Access. *International Journal of Legal Information*. 2024;52(2):155-165. doi:10.1017/jli.2024.37
20. Gafurova N., Yusupova F., Yusupov N., Protection of patients' rights during a pandemic // *Russian Law Journal*. 2023. №7S. Доступно на: <https://cyberleninka.ru/article/n/protection-of-patients-rights-during-a-pandemic>

References

1. О merah po dal'nejshemu reformirovaniyu sistemy zdravoohraneniya Ukaz Prezidenta Respubliki Uzbekistan, ot 26.02.2003 g. № UP-3214, Dostupno na: <https://lex.uz/uz/docs/-170143>

2. O merah po zaversheniyu eksperimenta i uglubleniyu reform v sisteme zdravoohraneniya Postanovlenie Kabineta Ministrov Respubliki Uzbekistan, ot 08.06.2004 g. № 264 Dostupno na: <https://lex.uz/uz/docs/-302557>
3. Westin A. Privacy and Freedom. — New York: Atheneum Dostupno na <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/>
4. Bygrave L.A. Data Privacy Law: An International Perspective. — Oxford University Press, 2014. Dostupno na: <https://dokumen.pub/data-privacy-law-an-international-perspective-9780199675555.html>
5. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008 Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888
6. Krysanova N. V. 2001. 04. 39. Maleina M. N. Lichnye neimushchestvennye prava grazhdan: ponyatie, osushchestvlenie, zashchita. M. : MZ Press, 2000. 244 s. Bibliogr. : S. 237-242 // Social'nye i gumanitarnye nauki. Otechestvennaya i zarubezhnaya literatura. Seriya 4. Gosudarstvo i pravo. 2001. №4. Dostupno na: <https://cyberleninka.ru/article/n/2001-04-39-maleina-m-n-lichnye-neimuschestvennye-prava-grazhdan-ponyatie-osuschestvlenie-zaschita-m-mz-press-2000-244-s-bibliogr-s-237-242>
7. Voigt, P. and Von dem Bussche, A. The EU General Data Protection Regulation (GDPR): A Practical Guide. 1st Edition, Springer International Publishing, Cham 2017, Dostupno na: <https://doi.org/10.1007/978-3-319-57959-7>
8. Daniel J. Solove, UNDERSTANDING PRIVACY, Harvard University Press, May 2008 Dostupno na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888
9. Nozimakhon, G., & Faringiz, Y. Analysis of International Legislation Regulating the Protection of Patients ' Rights. 2022, 5, 5–8. Dostupno na: <https://doi.org/10.31557/APJEC.2022.5.S1.5>.
10. Kodeks Respubliki Kazahstan ot 7 iyulya 2020 goda № 360-VI «O zdorov'e naroda i sisteme zdravoohraneniya» // IPS NPA RK. Dostupno na: <https://adilet.zan.kz/rus/docs/K2000000360> (Data obrashcheniya: 07.09.2025)
11. Ob utverzhdenii pravil osushchestvleniya sbora, obrabotki, hraneniya, zashchity i predostavleniya personal'nyh medicinskih dannyh sub"ektami cifrovogo zdravoohraneniya Priказ Ministra zdravoohraneniya Respubliki Kazahstan ot 14 aprelya 2021 goda № KR DSM -30. Zaregistrovan v Ministerstve yusticii Respubliki Kazahstan 15 aprelya 2021 goda № 22550. Dostupno na: <https://adilet.zan.kz/rus/docs/V2100022550/compare>
12. Grazhdanskij kodeks Respubliki Uzbekistan , Dostupno na: <https://lex.uz/docs/-180552>
13. YUsupova, F. "Medicinskie uslugi v epohu cifrovoj transformacii: pravovye aspekty telemediciny." LEGALITAS 4.4 (2025): 74-81.
14. Ob ohrane zdorov'ya grazhdan Zakon Respubliki Uzbekistan, ot 29.08.1996 g. № 265-I Dostupno na <https://lex.uz/mact/-26013>
15. Grazhdanskij kodeks Respubliki Uzbekistan, Dostupno na: <https://lex.uz/docs/-180552>
16. SC, I.F. (2013). Privacy and Confidentiality: The Doctor's Obligations. In: Beran, R. (eds) Legal and Forensic Medicine. Springer, Berlin, Heidelberg, Dostupno na: https://doi.org/10.1007/978-3-642-32338-6_147
17. Kodeks Respubliki Kazahstan ot 7 iyulya 2020 goda № 360-VI «O zdorov'e naroda i sisteme zdravoohraneniya» // IPS NPA RK. — <https://adilet.zan.kz/rus/docs/K2000000360> (Data obrashcheniya: 07.09.2025)
18. Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021. Licence: CC BY-NC-SA 3.0 IGO. Dostupno na: <https://www.who.int/docs/default-source/documents/gS4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf>

19. Qizi YFU. Telemedicine in the Digital Era: Navigating the International Legal Landscape to Expand Global Healthcare Access. International Journal of Legal Information. 2024;52(2):155-165. doi:10.1017/jli.2024.37
20. Gafurova N., Yusupova F., Yusupov N., Protection of patients' rights during a pandemic // Russian Law Journal. 2023. №7S. Dostupno na: <https://cyberleninka.ru/article/n/protection-of-patients-rights-during-a-pandemic>

Ф.У. Юсупова

PhD, доцент, Faringiz002@gmail.com, Өзбекстан Республикасы Өділет министрлігі жанындағы
Заңгерлердің біліктілігін арттыру және қайта даярлау институты, Ташкент, Өзбекстан

**МЕДИЦИНАЛЫҚ ҚЫЗМЕТТЕРДІ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА ПАЦИЕНТТІҢ
ЖЕКЕ ДЕРЕКТЕРІН ҚОРҒАУҒА АРНАЛҒАН ЗАҢДЫ КЕПІЛДІКТЕР: ШЕТЕЛДІК
ТӘЖІРИБЕ**

Түйін

Бұл мақалада халықаралық тәжірибені талдау негізінде медициналық қызметтерді цифрландыру аясында пациенттердің жеке деректерін қорғаудың құқықтық кепілдіктері қарастырылады. Электрондық медициналық жазбаларды, цифрлық платформаларды, телемедицина қызметтерін және автоматтандырылған денсаулық сақтау ақпараттық жүйелерін енгізу аясында дәстүрлі медициналық құпиялылық институтын трансформациялауға ерекше назар аударылады. Пациенттердің жеке деректері, соның ішінде денсаулық жағдайы, диагноз, тексеру нәтижелері және емдеу туралы ақпарат ақпараттың ерекше сезімтал санаты болып саналатыны және құқықтық, ұйымдастырушылық және техникалық қорғауды күшейтуді қажет ететіні дәлелденген. Халықаралық тәжірибеге сүйене отырып, медициналық деректерді өңдеуге пациенттің келісімін алу, мұндай деректерді мақсатты пайдалану, құпиялылықты, ақпараттық қауіпсіздікті, электрондық дерекқорларға қол жеткізуді бақылауды және пациенттің жеке деректерін өңдеу туралы ақпарат алу құқығы сияқты кепілдіктер сипатталған. Мақалада медициналық құпиялылықты жария етуге ресми тыйым салудан құқықтық, келісімшарттық, техникалық және ұйымдастырушылық тетіктерді қамтитын жеке медициналық деректерді қорғаудың кешенді моделіне көшу қажеттілігі атап өтілген. Цифрлық денсаулық сақтау саласындағы ұлттық заңнаманы жетілдіру және пациенттердің құқықтарын қорғау кепілдіктерін күшейту үшін халықаралық тәжірибенің маңыздылығы туралы қорытынды жасалған.

Кілттік сөздер: пациенттің дербес деректері, медициналық деректер, дәрігерлік құпия, медициналық қызметтерді цифрландыру, цифрлық денсаулық сақтау.

F.U. Yusupova

PhD, Associate Professor, Faringiz002@gmail.com, Institute for Retraining and Advanced
Qualifications of Legal Personnel under the Ministry of Justice of the Republic of Uzbekistan,
Tashkent, Uzbekistan

**LEGAL GUARANTEES FOR THE PROTECTION OF PATIENT PERSONAL DATA IN
THE CONTEXT OF DIGITALIZATION OF MEDICAL SERVICES: FOREIGN
EXPERIENCE**

Abstract

This article examines legal guarantees for protecting patient personal data in the context of digitalization of medical services, based on an analysis of international experience. Particular attention is paid to the transformation of the traditional institution of medical confidentiality in the context of the introduction of electronic medical records, digital platforms, telemedicine services, and automated healthcare information systems. It is substantiated that patient personal data, including information on health status, diagnosis, examination results, and treatment, are considered a particularly sensitive category of information and require

enhanced legal, organizational, and technical protection. Based on international experience, such guarantees as obtaining patient consent for the processing of medical data, the intended use of such data, ensuring confidentiality, information security, access control to electronic databases, and the patient's right to receive information about the processing of their personal data are described. The article emphasizes the need to move from a formal prohibition on disclosure of medical confidentiality to a comprehensive model for the protection of personal medical data, incorporating legal, contractual, technical, and organizational mechanisms. A conclusion is drawn on the significance of international experience for improving national legislation in the field of digital healthcare and strengthening guarantees for the protection of patient rights.

Keywords: patient's personal data, medical data, medical secrecy, digitalization of medical services, digital healthcare.