Электронный документооборот в здравоохранении

Концепция развития системы здравоохранения в Российской Федерации до 2020 г. содержит раздел 2.7 «Информатизация здравоохранения». В нем отмечается, что разработка и реализация программ информатизации здравоохранения в Российской Федерации ведется с 1992 г. На текущий период в стране созданы элементы информационно-коммуникационной инфраструктуры для нужд медицины, положено начало применению и распространению современных информационно-коммуникационных технологий в сфере здравоохранения. В проекте Концепции отмечалось, что целью информатизации системы здравоохранения является повышение доступности и качества медицинской помощи населению на основе автоматизации процесса ведения персональных медицинских данных, поддержки принятия решений и информационного взаимодействия.

Как показывают подсчеты зарубежных коллег, несмотря на издержки, связанные с внедрением информационных технологий, получаемая экономия средств (за счет стандартизации информационного обеспечения, повышения скорости принятия управленческих решений, экономии средств при оказании ряда услуг, внедрения электронных карт, электронных рецептов и др.) обязывает современное здравоохранение идти по пути активной информатизации.

К сведению

Проблема: - Слабая защита персональных данных пациента при их обработке в медорганизации, в том числе при введении электронного документооборота; недостаточная правовая регламентация внедряемых электронных систем

Проанализировав целый ряд нормативных актов, а также случаев из практики, необходимо рассмотреть отдельно электронную регистрацию и электронную медицинскую карту с точки зрения обеспечения защиты персональных данных пациентов и реализации их прав.

Безусловно, обеспечиваемая информатизацией защита конфиденциальных сведений от несанкционированного доступа (в части защиты персональных данных пациентов) заслуживает отдельного внимания. Многие из тех, кто был на приеме у врача, наверняка вспомнят, что на столе в его кабинете всегда лежит стопка медицинских карт, некоторые из них бывают открыты. Вследствие нехватки времени врачи часто продолжают заполнять карты предыдущих пациентов в присутствии следующих. Вольно или невольно посетитель может прочесть, что написано в чужой медицинской карте.

С правовой точки зрения мы имеем дело с несанкционированным доступом к личной информации. Согласно ст. 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Информатизация и оцифровка всех сведений о пациенте и его диагнозе способна минимизировать данный риск. Кроме того, такие действия позволят: сохранить действительную историю болезни (бумажный носитель может быть утрачен, испорчен, уничтожен по ошибке и пр.); врачам и медицинским организациям оперативно обмениваться информацией в условиях глобализации информационной базы.

Итак, переведение медицинской информации в **электронную форму позволит усилить ее защиту** (в том числе защиту биометрических данных) от несанкционированного доступа и от распространения (утечки). Однако обеспечить надлежащую защиту электронных данных не так просто. В

первоочередном порядке должны быть регламентированы вопросы автоматизированной обработки персональных данных пациентов, ведения первичной медицинской документации, имеющей важное юридическое значение, и медицинских архивов в электронном виде. Следует исключить дублирование документов на электронных и бумажных носителях, обеспечить равнозначность электронного и бумажного документооборота в организациях здравоохранения. Кроме того, нужно определить условия и порядок использования электронной цифровой подписи в здравоохранении.

ПРИМЕР

Несовершеннолетняя Елена К. состоит на учете в региональной поликлинике. Ее родители в силу специфики работы собираются переезжать в другой регион России. Мать Елены пришла в поликлинику, чтобы забрать карту дочери. Однако оказалось, что сделать это непросто. Сначала ей пришлось написать заявление на имя главного врача, затем дождаться конкретного дня, когда медработники подготовили все выписки из карты. Саму карту на руки женщине так и не отдали. По новому месту жительства семье придется снова вставать на учет, заводить новую карту и вклеивать в нее выписку.

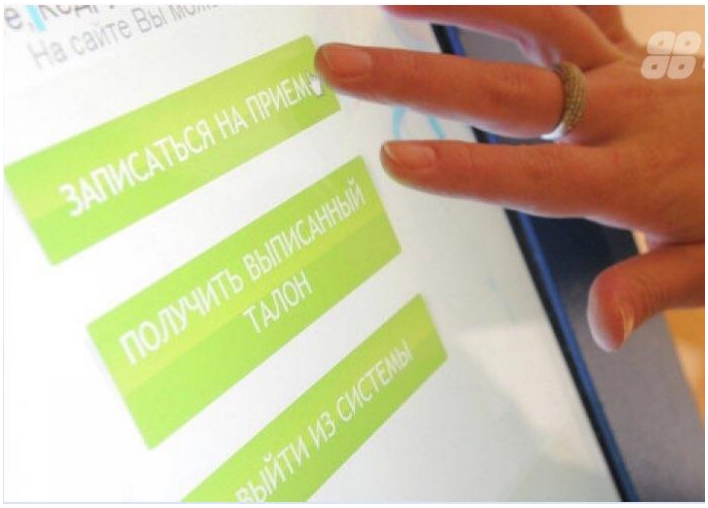
Ожидается, что информатизация здравоохранения в идеале должна сократить эту цепочку, вся информация о пациенте будет просто передаваться в другую медицинскую организацию в электронной форме.

В нашей стране отношения, связанные с обработкой персональных данных, осуществляемой государственными и муниципальными органами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, регулируются Законом No 152-ФЗ (ч. 1 ст. 1). В силу ст. 2 Закона No 152-ФЗ его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Стоит отметить, что отдельное регулирование статуса и механизмов проведения телемедицинских консультаций и консилиумов с

использованием телекоммуникационной сети Интернет в настоящее время отсутствует.

Электронная регистрация

Обязательными условиями записи на прием к врачу в электронной форме являются соблюдение информационной безопасности и защита персональных данных в соответствии с требованиями законодательства. Согласно ч. 1 ст. 9 Закона No 152-ФЗ субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Оно может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя проверяются оператором. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных также возлагается на оператора (ст. 9).



Разберемся с тем вопросом, кто является **оператором** в медицинской организации. В ст. 3 Закона No 152-ФЗ дается определение понятия «оператор» — это государственный орган, муниципальный орган,

юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. По смыслу норм закона оператором может считаться сама медицинская организация (как организатор электронной регистрации), которая и ведет сбор, обработку и хранение персональных данных.

На практике, если речь будет идти о частной клинике, оператором будет юридическое лицо, предоставляющее медицинские услуги. Если мы говорим о бюджетном медицинском учреждении, оператором выступает уполномоченный орган в лице Минздрава и его отдельных подразделений, отвечающих за организацию автоматизации процессов.

В соответствии со **ст. 7 Закона No 152-ФЗ операторы и иные лица**, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Таким образом, рекомендуем оператору обработки персональных данных (лицу, осуществляющему сбор, обработку и хранение персональных данных) при осуществлении электронной регистрации пациента на прием к врачу предусмотреть disclaimer (объявление об ограничении ответственности, обращающее на себя внимание пользователя), имеющий определенное содержание.

Пока остается без ответа вопрос о правовой квалификации электронной регистрации на прием к врачу. Нам представляется, что электронную регистрацию на прием к врачу надлежит квалифицировать как акцепт на оказание медицинских услуг. В соответствии с п. 1 ст. 438 ГК РФ акцептом признается ответ лица, которому адресована оферта (предложение), о ее принятии. Акцепт 5 должен быть полным и безоговорочным. Таким образом,

пациент, осуществляя электронную регистрацию на прием к врачу, акцептует оферту медицинской организации на оказание медицинских услуг.

Электронная медицинская карта

Первой попыткой регламентирования электронных персональных медицинских записей и внесения таких записей в электронную медицинскую карту (ЭМК) стал приказ Ростехрегулирования от 27.12.2006 No 407-ст (ГОСТ Р 52636–2006). Позднее был принят документ «Основные разделы электронной медицинской карты» (утв. Минздравом России от 11.11.2013 No 18–1/1010). В документе представлены требования к стандартизации электронных медицинских данных и структуре ЭМК. Иными словами, первые шаги были сделаны достаточно давно. Дело за финансированием проекта и внедрением его на местах.

Как указано в документе, ЭМК ориентирована на пациента (потребителя) и должна содержать информацию, относящуюся ко всем видам медицинского обеспечения, включая вспомогательные и экстренные услуги. В этом ЭМК отличается от карты, ориентированной на поставщика услуг, или исключительно эпизодического учета. ЭМК содержит результаты наблюдений (что произошло), мнения (решения о том, что должно произойти) и планы лечения (планы относительно того, что должно произойти).

Сама по себе специализированная информация, например в виде графических изображений, руководств или алгоритмов поддержки принятия решения, как правило, не является частью ЭМК. Обобщает информацию, содержащуюся в ЭМК, медицинский работник, для этого ЭМК должна иметь соответствующие интерфейсы. ЭМК принимает и хранит диагностические и другие тестовые данные и одновременно является многофункциональной базой клинических данных, необходимых для лечения, поддержки принятия решений медицинским работником, научно- исследовательских целей, работы статистических бюро и других потребителей. ЭМК фактически

представляет собой долговременный накопитель информации о том, что произошло у пациента или было сделано для него.

КСТАТИ

В ЭМК должны храниться сведения о предоставлении и/или отзыве информированного добровольного согласия пациента, а также сведения о лицах, которым могут быть сообщены биометрические данные пациента, включая сведения о проведенных исследованиях и их результатах, а также о поставленных диагнозах.

Данные ЭМК позволяют контролировать правильность организации лечебно-диагностического процесса, составлять рекомендации по дальнейшему обследованию и лечению больного и диспансерному наблюдению за ним, получать информацию, необходимую для установления инвалидности, а также выдачи справочного материала по запросам ведомственных учреждений.

Недоработки законодательства

К сожалению, ни один из нормативных документов, как уже принятых, так и находящихся на стадии обсуждения в качестве законодательных инициатив, не содержит норм, регламентирующих порядок реализации прав пациентов, установленных в ст. 18–26 Закона об охране здоровья, при информатизации здравоохранения. Рассмотрим, к примеру, права на охрану здоровья, обеспечивающиеся оказанием доступной медицинской помощи. Все программы информатизации предполагают упрощение реализации права, следовательно, предполагают сделать медицинскую помощь более доступной.

Однако обыватели при обращении в государственную поликлинику в настоящее время сталкиваются со следующим. Допустим, электронная запись на прием проводится через интернет (один из способов электронной записи). Существуют сайты, где можно записаться на прием к врачу и получить талон. Если гражданин живет в мегаполисе, эта схема обычно работает. Однако если он живет лишь немного дальше (на личном примере

— не далее 30 км от МКАД), то талон к врачу он сможет получить только так: прийти в регистратуру не позже 6 утра (при этом медорганизация начинает работу с восьми) и занять очередь. В регистратуре производится запись и выдается талон к специалисту. Самое интересное, что такая запись почему-то считается электронной (!), но сайт не работает.

Далее, ни один из законов и подзаконных актов не уточняет, каким образом при переводе всех карт в электронный формат будет реализовано право пациента на информацию о состоянии здоровья. Будет ли это возможность ознакомиться с электронной версией медицинской карты на удаленном доступе (например, по аналогии с порталом «Госуслуги»)?

Однако при высокой степени развития киберпреступности в стране велик риск утечки конфиденциальной информации, поэтому должны быть разработаны и внедрены отдельные способы и методы защиты, а также отдельные способы аттестации программ защиты от всех степеней угроз. К сожалению, в действующих регламентах Роскомнадзора или приказах ФСБ России об организации защиты и способах защиты отдельных категорий персональных данных не уделено внимания информатизации здравоохранения.

Ответственность

Статья 5 Закона No 152-ФЗ регламентирует принципы обработки персональных данных. Согласно ее положениям обработка персональных данных должна осуществляться на законной и справедливой основе, ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями их сбора. Не допускается также объединение баз данных, содержащих персональные данные, которые обрабатываются в целях, несовместимых между собой.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки данных. Оператор должен

принимать необходимые меры (либо обеспечивать их принятие) по удалению или уточнению неполных либо неточных данных.

Персональные данные хранятся в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен особо федеральным законом или договором. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Условия обработки персональных данных прописаны в ст. 6 Закона No 152-ФЗ. Статья 24 Закона устанавливает, что лица, виновные в нарушении требований этого нормативного документа, несут предусмотренную законодательством РФ ответственность — гражданскую, административную и уголовную.

Гражданская ответственность лица, виновного в распространении персональных данных, предусматривает возмещение причиненного вреда субъекту персональных данных. В частности, речь может идти о возмещении морального вреда. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных данным Законом, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Административная ответственность предусмотрена ст. 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)» КоАП РФ. Эта статья — специальная, она регламентирует ответственность специальных субъектов. В соответствии с ней нарушение установленного законом порядка сбора, хранения, использования или распространения

информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от 300 до 500 руб.; на должностных лиц — от 500 до 1000 руб.; на юридических лиц — от 5000 до 10 000 руб. Особое внимание должно быть обращено на то обстоятельство, что субъектом административной ответственности является не только определенное физическое лицо, допустившее нарушение, но и организация в целом.

ВАЖНО

Обработке подлежат только те персональные данные, которые отвечают целям их обработки

Кроме гражданской и административной, существует также уголовная ответственность: ст. 137 УК РФ закрепляет наступление уголовной ответственности за нарушение неприкосновенности частной жизни. Рассмотрим эту статью подробнее. Часть 1 указанной статьи определяет меру наказания за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

СПРАВКА

Санкция ч. 1 ст. 137 УК РФ альтернативная, выбор наказания поставлен в зависимость от характера преступления, предварительного и последующего поведения виновного, его личности и многого другого.

Санкция указанной ч. 1 следующая: **штраф в размере до 200 000 руб**. или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательные работы на срок до трехсот шестидесяти часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет с лишением права занимать

определенные должности или заниматься определенной деятельностью на срок до трех лет.

Объективная сторона этого преступления, как следует из диспозиции данной нормы, характеризуется следующими действиями в альтернативе или совокупности: незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия; незаконное распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия; распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Следует отметить, что преступление будет **считаться оконченным с момента сбора или распространения таких сведений, независимо от наступивших последствий**. Субъект преступления является общим. Непосредственным объектом преступления будет частная жизнь лица. Предметом же — любые сведения, составляющие личную или семейную тайну лица. Они разнообразны, это может быть информация, касающаяся имущественного положения лица, его сексуальной ориентации, духовной жизни, здоровья и др.

Часть 2 ст. 137 УК РФ содержит квалифицированный состав этого преступления. Квалифицирующим признаком выступает использование служебного положения. Следует не забывать о том, что наказание при таких условиях соответственно выше. Санкция ч. 2 ст. 137 УК РФ, более интересующая нас для целей раскрытия заявленной темы, альтернативно предусматривает: штраф в размере от 100 000 до 300 000 руб. или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет; лишение права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет; принудительные работы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового; арест на срок до шести месяцев; лишение свободы на срок

до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Основное доказательство совершения такого преступления — **умысел**.

Таким образом, информатизация здравоохранения на текущий момент является насущной, разумной, актуальной и реализуемой задачей. Тем не менее имеются многочисленные пробелы и недоработки, а также сложности реализации этой программы на местах, что ведет к нарушению прав пациента. Авторы настоящей статьи надеются, что информатизация здравоохранения и ее электронные инициативы все же приведут к улучшению качества и повышению доступности медицинской помощи, а также сократят сроки принятия тех или иных врачебных решений.