Ассоциация медицинского права Санкт-Петербурга

«Правовые риски реализации нового закона по вопросам применения информационно-телекоммуникационных технологий и введения электронных форм документов в сфере здравоохранения в деятельности медицинских организаций"

Акулин Игорь Михайлович, д.м.н., президент Ассоциации медицинского права Санкт-Петербурга, руководитель магистерской программы по медицинскому праву, зав каф. организации здравоохранения и медицинского права СПбГУ

Стратегия перехода

На Пленарном заседании Санкт-Петербургского экономического Форума 2017 В.В. Путин сказал: «К середине следующего десятилетия, уважаемые друзья, мир, совершенно очевидно, будет совершенно другим. Не замечать, игнорировать происходящие процессы – значит оказаться на обочине развития. А чтобы быть лидерами, нужно самим формировать эти изменения.»

Ведущие страны мира ищут источники роста, и ищут в использовании, в капитализации колоссального технологического потенциала, который уже имеется и продолжает формироваться прежде всего в цифровых и промышленных технологиях, робототехнике, энергетике, биотехнологиях и медицине, в других сферах. Открытия в этих областях способны привести к настоящей технологической революции, к взрывному росту производительности труда.

Государство не может снять с себя ответственность за сохранение таких основополагающих прав человека как право на жизнь и охрану здоровья, а это является недопустимым. Это связано с тем, что медицинская деятельность напрямую связана с объектом оказания медицинских услуг – правоотношениями в обеспечении жизни и здоровья граждан.

В связи с этим формирование новой стратегии Государства РФ направленной на создание Национальной системы здравоохранения работающей по единым правилам, стандартам, порядкам включающей в себя как государственную, муниципальную, так и частную систему здравоохранения является актуальной.

Государство не должно передавать кому-либо функций по принятию базовых стандартов осуществления медицинской деятельности как в сфере профилактики, так и лечения и особенно в сфере электронного документооборота, с целью защиты персональных данных и стратегии государственной безопасности.

Публичная значимость медицинской деятельности

Отражена в решении Конституционного суда, в Постановлении Конституционного Суда РФ от 03.06.2004 N *11-П "По делу о проверке конституционности положений подпунктов 10, 11 и 12 пункта 1 статьи 28, пунктов 1 и 2 статьи 31 Федерального закона «О трудовых пенсиях в Российской Федерации».*

***В нем приводится перечень* особенностей медицинской деятельности:**

- обязанность медицинских работников при оказании экстренной и неотложной помощи безотлагательно осуществлять медицинскую деятельность;

- наличие у медицинских работников власти особого рода (профессиональной власти) в отношении пациента (в отдельных случаях медицинская помощь может оказываться даже против воли пациента);

- наличие доверия в отношениях медицинского работника и пациента при их фактическом неравенстве;

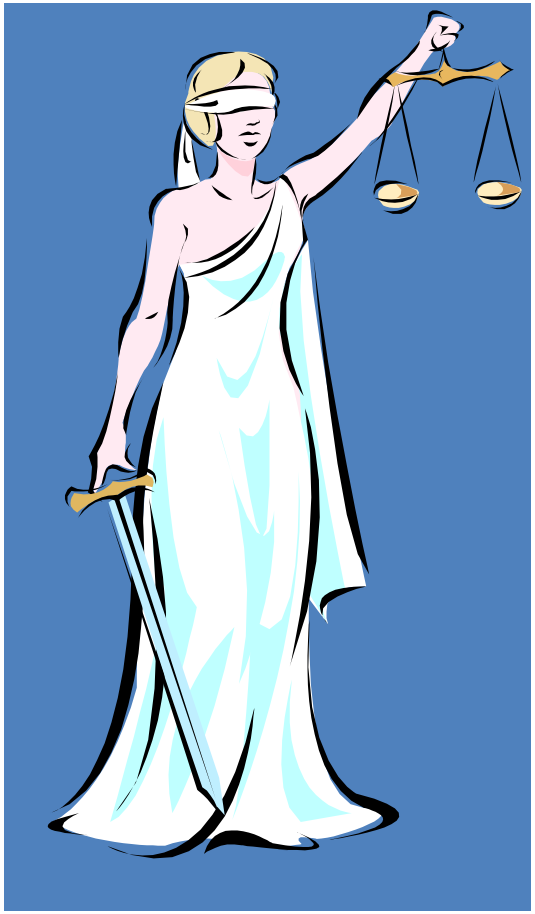
- неопределенность труда медицинских работников в части выбора адекватных для пациента и его болезни средств (риск медицинского вмешательства);

- независимость в принятии своих решений медицинскими работниками, возможность действовать вне указаний работодателя.

Публичная значимость медицинской деятельности

Таким образом деятельность медицинского работника с одной стороны обладает властными полномочиями по отношении пациента, в силу особого профессионального статуса и знаний, с другой стороны эта публичная деятельность носит рисковый характер и нуждается в особой форме контроля и правовой защите одновременно.

В связи с предстоящей «цифровизацией» медицинских технологий и системы управления отрасли возникает целый ряд правовых рисков.



В настоящее время практически все отношения, связанные с реализацией права на охрану здоровья, могут быть предметом судебной защиты.

ФЕДЕРАЛЬНЫЙ ЗАКОН (проект)
«О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационно-телекоммуникационных технологий и введения электронных форм документов в сфере здравоохранения».

Основные моменты реформы

- **Предусматривается создание Единой государственной информационной системы в сфере здравоохранения**

- **предусматривается возможность выдачи рецептов на лекарственные препараты, в том числе рецепты на лекарственные препараты, содержащие назначение наркотических средств или психотропных веществ, справок и рецептов на медицинские изделия, в форме электронного документа**

- **вводится возможность оказания медицинской помощи с применением телемедицинских технологий путем проведения консультаций и консилиумов, обеспечивающих дистанционное взаимодействие врачей между собой, врача и пациента или его законного представителя, а также дистанционный мониторинг состояния здоровья пациента.**

- **в дополнение к возможности создания и ведения Федеральных регистров лиц, инфицированных ВИЧ, больных туберкулезом или страдающих жизнеугрожающими и хроническими прогрессирующими редкими (орфанными) заболеваниями, приводящими к сокращению продолжительности жизни или инвалидности предусматривается возможность создания иных федеральных регистров лиц, страдающих отдельными заболеваниями.**

Основные правовые риски

- **Юридическая значимость электронных документов:**

1. **Защита персональных данных пациента (безопасность врачебная тайна), доступность информации для пациента, конфиденциальность данных, врачебная тайна.**
2. **Квалифицированная электронная подпись (юридическое значение).**
3. **Федеральный обмен медицинскими данными, без согласия пациента, в интересах преемственности, кооперации, в принятии адекватного медицинского решения в системе ОМС, ДМС, экстренной и неотложной медицины, МЧС и других ситуаций.**
4. **Доступность информации для третьих лиц (работодатель, наследники и т.д.), субъектов здравоохранения. Правоохранительные органы, следствие, порядок предоставления информации.**

Основные правовые риски (продолжение)

- Юридическая значимость электронных документов

5. **Отказ пациента** от участия в системе цифрового документооборота (религиозные мотивы, физическая немощность, дети, инвалиды, иностранные граждане и др.).
6. Отсутствие подзаконных актов МЗ РФ, ФФОМС, ФФС и др. связанные с документооборотом в сфере здравоохранения и **необходимость внесения в огромное количество документов связанных, как с Договорами так и с техническими проблемами.**
7. Отдельные возможности, обеспечиваемые введением электронного документооборота (например, возможность **автоматической проверки** соответствия выбранной тактики диагностики и лечения действующим **стандартам**) могут создать определённые проблемы на уровне правоприменительной практики (например, при установлении **ответственности медицинского работника и организации**)
8. Внесение дополнений в **образовательные стандарты подготовки медицинских работников,** связанных с цифровым документооборотом.

Основные технические меры по обеспечению информационной безопасности и защиты персональных данных

1. Использование электронной цифровой подписи.

2. Использование электронных средств идентификации врача и пациента (универсальная электронная карта гражданина Российской Федерации)

   Но с 1 января 2017 года универсальная электронная карта как обязательный инструмент предоставления государственных и муниципальных услуг отменена Федеральным законом от 28.12.2016 N 471-ФЗ

Что такое электронная подпись, юридическое определение.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (п.1 ст.2)

1 июля 2013 года утратил силу Федеральный закон от 10.01.02 № 1-ФЗ «Об электронной цифровой подписи» и вступил в силу

Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи».

Федеральный закон от 06.04.11 № 63-ФЗ «Об электронной подписи»

Новый закон ввел три вида электронной подписи:

- **простая (ЭП),**
- **усиленная неквалифицированная (НЭП),**
- **усиленная квалифицированная (КЭП)**

Усиленная квалифицированная электронная подпись (п.4 ст.5 63-ФЗ)

- **Получена в результате криптографического преобразования информации с использованием ключа электронной подписи;**
- **Позволяет определить лицо, подписавшее электронный документ;**
- **Позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;**
- **Создается с использованием средств электронной подписи**
- **Ключ проверки электронной подписи указан в квалифицированном сертификате;**
- **Для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом № 63-ФЗ.**

Усиленная квалифицированная электронная подпись

- **В соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) в случаях, если федеральными законами и иными нормативными правовыми актами, вступившими в силу до 1 июля 2013 года, предусмотрено использование электронной цифровой подписи, используется усиленная квалифицированная электронная подпись.**

Квалифицированная электронная подпись в новом законе

Новый закон предусматривает возможность создания и ведения целой серии электронных медицинских документов, подписанных усиленной квалифицированной электронной подписью:

- **Рецепты на лекарственные препараты**
- **Рецепты, содержащие назначение наркотических средств или психотропных веществ**
- **Информированное добровольное согласие на медицинское вмешательство или отказ от медицинского вмешательства**
- **Направляемые пациенту по его запросу медицинские документы, включая выписки из них, и копии медицинских документов, в том числе в форме электронных документов, подписанных усиленной квалифицированной электронной подписью врача (фельдшера, акушера)**

Преимущества КЭП

- **Безопасность использования: подделать КЭП сложно, намного сложнее, чем подделать рукописную подпись;**

- **Экономия времени и возможность взаимодействия с лицами, находящимися на значительном расстоянии**

Значение КЭП при оценке электронных медицинских документов

- **КЭП может обеспечить допустимость документа в качестве доказательства в случаях, когда нормативными актами или условием договора не предусмотрены требования к оформлению документа**

  документы, подписанные усиленной квалифицированной ЭП, признаются равнозначными бумажному документу, подписанному собственноручно [4, п. 1 ст. 6 Федеральным законом от 06.04.2011 N 63-ФЗ]

- **КЭП упрощает установление авторства документа;**

  владелец КЭП не может отказаться от своей подписи под документом, так как ключ, необходимый для создания КЭП, имеется лишь у владельца подписи

  КЭП обеспечивает контроль целостности документа: в случае любого случайного или преднамеренного изменения документа КЭП станет недействительной, так как КЭП вычисляется по специальному алгоритму на основании исходного состояния документа.

Но!!!

Ключ КЭП может быть несанкционированно использован или похищен!!!

Проблемы в применении КЭП

- **Недостаточный уровень информационной культуры населения, отсутствие навыков работы в сети Интернет**
- **Низкий уровень доверия к инновационным технологиям со стороны населения**
- **Отсутствие в организациях локальных актов и/или неэффективное применение организационных мер, направленных на ограничение прав доступа к информации**
- **Низкий уровень осведомлённости сотрудников о правилах работы с паролями и ключами**
- **Преступления в компьютерной сфере.**

Единая государственная информационная система в сфере здравоохранения

- **Концепция создания единой государственной информационной системы в сфере здравоохранения была утверждена Приказом Минздравсоцразвития РФ от 28.04.2011 N 364**
- **Новым законом предусматривается создание Единой системы, определяется ее оператор, состав обрабатываемых в ней сведений, правовые основы ее функционирования и информационного взаимодействия с иными информационными системами, а также поставщики и пользователи информации.**
- **Положение о Единой системе, в том числе порядок доступа к Единой системе, порядок и сроки предоставления информации в Единую систему, а также источники и состав сведений, формирование, обработка которых и доступ к которым осуществляются с использованием Единой системы, утверждаются Правительством Российской Федерации.**

Перечень видов информации, предоставляемой и обрабатываемой в Единой системе, определен в новом законе исчерпывающим образом.

- **Участниками информационного взаимодействия являются:**
- **1) уполномоченный федеральный орган исполнительной власти;**
- **2) поставщики информации:**
- **федеральные органы исполнительной власти;**
- **ФФОМС и ТФОМС в части, касающейся персонифицированного учета в системе ОМС;**
- **Пенсионный фонд Российской Федерации;**
- **Фонд социального страхования Российской Федерации;**
- **уполномоченные органы государственной власти субъектов Российской Федерации;**
- **органы местного самоуправления;**
- **медицинские организации;**
- **организации, реализующие профессиональные образовательные программы медицинского образования и фармацевтического образования;**
- **иные органы и организации, определяемые Правительством Российской Федерации;**

- **3) пользователи информации, к которым относятся поставщики информации и граждане.**

Защита персональных данных, врачебная тайна.

- **Основной риск: защита персональных данных, врачебная тайна.**

  Средства защиты персональных данных в информационных системах:
- **применение ключей электронной подписи и шифрование данных;**
- **Обезличивание персональных данных, передаваемых для централизованной обработки;**
- **Принятие правовых и организационных мер, направленных на ограничение и разграничение доступа к информации!**

Виды информации в Единой системе

- **Новый закон среди видов информации, предоставляемой и обрабатываемой в Единой системе, предусматривает сведения, обрабатываемые в процессе ведения персонифицированного учета в сфере здравоохранения.**

- **Персонифицированный учет при осуществлении медицинской деятельности - обработка персональных данных о лицах, которые участвуют в оказании медицинских услуг, и о лицах, которым оказываются медицинские услуги (п.1 ст.92 323-ФЗ)**

- **Сведения о лицах, которые участвуют в оказании медицинских услуг, и о лицах, которым оказываются медицинские услуги, относятся к информации ограниченного доступа и подлежат защите в соответствии с законодательством РФ (п.4 ст.92 323-ФЗ).**

Статья 16, Защита информации ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ

- 1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:
- 1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- 2) соблюдение конфиденциальности информации ограниченного доступа;
- 3) реализацию права на доступ к информации.

Зарубежный опыт: австрийский закон ELGA-Gesetz от 2012г.

- **Австрийская национальная система** Elektronische Gesundheitsakte (ELGA) обеспечивает связь между поставщиками медицинских услуг, такими как больницы, частные медицинские практики, дома-интернаты для инвалидов и престарелых, аптеки.
- **Ключевым компонентом** ELGA-Gesetz является **соблюдение прав пациентов** в отношении того, как используются данные. **Пациенты могут регулировать параметры использования через центр контроля доступа.** Это позволяет им видеть, кто ознакомился с их данными, и **решить, следует ли им расширить или сократить время доступа, запретить доступ к** определенным документам. **Пациенты могут принять решение о полном выходе** из системы ELGA или об участии только в отдельных приложениях, таких как услуги электронных рецептов

Врачебная тайна

- **Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну (ч.1 ст.13 323-ФЗ).**
- **Часть 3 ст. 13 в качестве условия раскрытия врачебной тайны ставит письменное согласие пациента.**
- **Часть 4 ст. 13 содержит закрытый перечень случаев, когда врачебная тайна может быть раскрыта без согласия пациента.**
- **Таким образом, информация, к которой имеется доступ у поставщиков информации Единой сети (ФОМС, органы государственной власти, медицинские организации и др.) в отсутствии письменного согласия пациента должна быть обезличенной!!!**

ПРАВО НА УВАЖЕНИЕ ЧАСТНОЙ ЖИЗНИ

- **РАСКРЫТИЕ МЕДИЦИНСКИМИ ОРГАНИЗАЦИЯМИ ИНФОРМАЦИИ О СОСТОЯНИИ ЗДОРОВЬЯ ПАЦИЕНТОВ ДРУГИМ МЕДИЦИНСКИМ ОРГАНИЗАЦИЯМ, ОРГАНАМ СОЦИАЛЬНОГО СТРАХОВАНИЯ, ПРОКУРАТУРЕ И ГОСУДАРСТВЕННЫМ ОРГАНАМ КОНТРОЛЯ – ВМЕШАТЕЛЬСТВО В ПРАВО НА УВАЖЕНИЕ ЧАСТНОЙ ЖИЗНИ!!!**

Позиция Европейского суда по правам человека

- **Личная информация, относящаяся к пациенту, относится к сфере его или ее личной жизни (см. "Y.Y. против Российской Федерации" от 23.02. 2016г., "I. против Финляндии" от 17.08. 2008 г., "L.L. против Франции").**

- **Защита персональных данных, особенно медицинских данных, имеет фундаментальное значение для осуществления лицом права на уважение личной и семейной жизни, гарантированного ст. 8 Конвенции. Важно не только соблюдать чувство уединения пациента, но и сохранить его или ее доверие к медицинской профессии и медицинскому обслуживанию в целом (см. "Y.Y. против Российской Федерации" от 23.02.2016г., "Z. против Финляндии" от 25.02.1997 г., "P. и S. против Польши" от 30.10. 2012 г., "L.H. против Латвии" от 29.04. 2014 г.).**

- **Без такой защиты подобная информация личного и интимного характера нуждающихся в медицинской помощи лиц не может быть раскрыта, в том числе для получения адекватного лечения и вообще медицинской помощи, даже при угрозе их собственному здоровью и, в случае инфекционных заболеваний, здоровью других людей.**
  В связи с этим внутригосударственное законодательство должно предоставлять соответствующие гарантии для предотвращения передачи или разглашения персональных данных о состоянии здоровья, (см. "Y.Y. против Российской Федерации" от 23.02.2016г., "Z. против Финляндии").

Сведения по запросу Прокуратуры.

Кроме того, предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается не только по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, но и **по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора.** Так, согласно статье 26 Федерального закона от 17 января 1992 года N 2202-1 "О прокуратуре Российской Федерации" предметом надзора со стороны прокуратуры является соблюдение прав и свобод человека и гражданина, в частности, органами управления и руководителями коммерческих и некоммерческих организаций, а значит, и учреждений здравоохранения. При этом в силу статьи 27 данного Федерального закона прокурор при проверке заявления, жалобы или иного сообщения о нарушении прав и свобод человека и гражданина **использует все имеющиеся у него полномочия, включая получение доступа к необходимой для осуществления прокурорского надзора информации,** доступ к которой ограничен в соответствии с федеральными законами, в частности осуществляет обработку персональных данных (пункт 7.1 части 2 статьи 10 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных"). **На это полномочие прокурора указывается также в пункте 3 части 4 статьи 13 Федерального закона "Об основах охраны здоровья граждан в Российской Федерации" (в редакции Федерального закона от 23 июля 2013 года N 205-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с уточнением полномочий органов прокуратуры Российской Федерации по вопросам обработки персональных данных").**

Допустимость разглашения врачебной тайны в интересах государства и общества.

В постановлении от 6 июня 2013 года по делу "Авилкина и другие против России" Европейский Суд по правам человека напомнил, что интерес пациента и общества в целом в защите конфиденциальности медицинских данных может быть перевешен интересом в расследовании и преследовании преступлений, а также гласности судебного разбирательства, если доказано, что эти интересы имеют более серьезное значение; обязательства государства создавать гарантии судебной защиты от посягательств права на жизнь или личную неприкосновенность в медицинской сфере не ограничиваются только уголовно-правовыми средствами и могут включать правила о гражданско-правовом возмещении, в частности о компенсации ущерба, а равно о мерах дисциплинарного взыскания (постановление от 30 октября 2012 года по делу "Е.М. и другие против Румынии").

Допустимость разглашения врачебной тайны в интересах государства и общества.

Международное право и конституционные нормы, таким образом, не устанавливают конкретных процедур, в рамках которых заинтересованное лицо может ознакомиться с информацией, содержащей медицинскую тайну иного лица.

Соответственно, федеральный законодатель обладает определенной свободой усмотрения при создании правовых механизмов, которые - при соблюдении надлежащего баланса защищаемых Конституцией Российской Федерации ценностей - позволяли бы заинтересованному лицу осуществлять эффективную защиту (в том числе судебную), как принадлежащих ему имущественных прав и нематериальных благ, так и права на человеческое достоинство (после смерти тоже).

КОНСТИТУЦИОННЫЙ СУД РОССИЙСКОЙ ФЕДЕРАЦИИ ОПРЕДЕЛЕНИЕ от 16 июля 2013 г. N 1176-О ОБ ОТКАЗЕ В ПРИНЯТИИ К РАССМОТРЕНИЮ ЖАЛОБЫ ГРАЖДАНИНА КРУГЛОВА АЛЕКСАНДРА ГЕННАДЬЕВИЧА НА НАРУШЕНИЕ ЕГО КОНСТИТУЦИОННЫХ ПРАВ ПУНКТОМ 4 ЧАСТИ 2 СТАТЬИ 10 ФЕДЕРАЛЬНОГО ЗАКОНА "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

В своей жалобе гражданин А.Г. Круглов оспаривает конституционность пункта 4 части 2 статьи 10 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных", в соответствии с которым обработка указанных в части 1 данной статьи специальных категорий персональных данных допускается в случае, когда она осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

А.Г. Круглов обратился в суд с требованием обязать "Самарский психоневрологический диспансер" удалить его незаконно обрабатываемые персональные данные. Ленинский районный суд города Самары, руководствуясь пунктом 4 части 2 статьи 10 Федерального закона "О персональных данных", решением от 25 января 2013 года, оставленным без изменения судом апелляционной инстанции, отказал заявителю в удовлетворении указанных требований.

По мнению заявителя, оспариваемое законоположение допускает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и не предусматривает условия прекращения обработки его персональных данных. В связи с этим заявитель просит признать оспариваемую норму не соответствующей статьям 2, 18, 19 (части 1 и 2), 21 (часть 1), 23 (часть 1), 24 (часть 1), 45 (часть 1), 46 (часть 1), 55 (часть 2) и 56 (часть 3) Конституции Российской Федерации.

Обработка персональных данных, законность использования без согласия пациента.

Конституционный Суд Российской Федерации, не находит оснований для принятия жалобы к рассмотрению.

Федеральный закон "О персональных данных", принятый в целях обеспечения 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, устанавливает принципы и условия обработки персональных данных (глава 2).

В силу статьи 5 данного Федерального закона такая обработка должна ограничиваться достижением конкретных, заранее определенных и законных целей; *не допускается обработка персональных данных, несовместимая с целями сбора персональных данных; содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки;* ***обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки (части 2, 4 и 5).***

Обработка персональных данных, законность использования без согласия пациента.

По общему правилу, предусмотренному частью 1 статьи 10 указанного Федерального закона, обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается.

Исключения из этого правила носят ограниченный характер, к их числу относится оспариваемая заявителем возможность обработки персональных данных в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну (пункт 4 части 2 статьи 10).

Таким образом, оспариваемое законоположение позволяет хранить информацию о состоянии здоровья граждан исключительно в целях реализации их права на охрану здоровья и медицинскую помощь, при этом конфиденциальность персональных данных обеспечивается врачебной тайной, а потому оно не может рассматриваться как нарушающее конституционные права заявителя в указанном им аспекте.

ФЕДЕРАЛЬНЫЙ АРБИТРАЖНЫЙ СУД ЦЕНТРАЛЬНОГО ОКРУГА
ПОСТАНОВЛЕНИЕ от 3 сентября 2013 г. по делу N А35-10589/12 Цифровая подпись.

В соответствии со статьей 2 ФЗ от 06.04.2011 N 63-ФЗ "Об электронной подписи" электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Согласно статье 10 названного Закона при использовании усиленных электронных подписей участники электронного взаимодействия обязаны: обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия; уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении; не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена; использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей их проверки средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

Ассоциация медицинского права Санкт-Петербурга

Санкт-Петербургский государственный университет

Спасибо за внимание!

Дополнительные риски:

1. Участие третьих лиц в обработке ПД - практически при любом случае передачи третьим лицам РКН требует соблюдения ч. 3 ст. 6 (наличие договора об обработке данных с указанием ряда дополнительных реквизитов). Помимо этого общая проблема - как разумно организовать соблюдение всех требований закона в случаях, когда данные должны передаваться для обработки многим третьим лицам.

2. Актуально для тех организаций, которые сотрудничают с зарубежными организациями и (или) действуют за рубежом полностью или в части - требование о локализации персональных данных, содержащееся в ч. 5 ст. 18 ФЗ "О персональных данных" + вопросы трансграничной передачи ПД, особенно в страны, не обеспечивающие их адекватной защиты (например, США).

3. Сохраняющаяся проблема - всегда ли обезличивание может рассматриваться как действие, в результате которого информация теряет режим персональных данных. Проблема в том, что сам закон оперирует понятием "обезличенные персональные данные" и есть версия, что из методики РКН (Роскомнадзор) по обезличиванию ПД следует, что обратимое обезличивание (когда данные могут быть обратно расшифрованы) не приводит к тому, что данные перестают быть персональными.

Дополнительные риски:

4. Общие практические проблемы реализации требований к **внутренней документации и процедурам** (помимо согласия и прочих вопросов), указанных в ст. 18.1 и ст. 19 ФЗ "О персональных данных".

5. Как реализовывать на практике эффективным образом требование закона о том, что согласие на обработку ПД должно быть конкретным, информированным и осознанным. Например, нам по практике известно, что РКН сейчас считает, что одно согласие может содержать только одну цель обработки ПД (это противоречит сложившейся реальной практике операторов), иначе субъекту как бы навязываются другие цели и он может быть лишен выбора здесь. Как вариант - включать в тексты согласия поля с отдельной "галочкой" или подписью.

6. Общее обсуждение "Больших данных" в медицине, - вопрос, который полностью пересекается и с общей тематикой электронной информации в медицине, и с вопросами ПД.

Дополнительные риски:

Статья 18.1. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом

[Закон РФ "О персональных данных"] [Глава 4] [Статья 18.1]

1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:

1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

Дополнительные риски:

5) **оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;**

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

2. **Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных**, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

3. Правительство Российской Федерации устанавливает перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, **операторами, являющимися государственными или муниципальными органами.**

4. Оператор обязан представить документы и локальные акты, указанные в части 1 настоящей статьи, и (или) иным образом подтвердить принятие мер, указанных в части 1 настоящей статьи, по запросу уполномоченного органа по защите прав субъектов персональных данных.

Дополнительные риски:

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 22.02.2017) "О персональных данных"> Глава 4. Обязанности оператора> Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2. Обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы