



Персональные данные пациентов в медицинских организациях: требования к обработке и ответственности

Семенов Дмитрий Сергеевич
Заместитель начальника отдела информационной
безопасности ГУЗ «МИАЦ»,
тел. 384-194 доб.11, e-mail: d.semenenko@mz73.ru

вторник, 3 марта 2020 г.



Медицинские организации в силу законодательства являются операторами персональных данных своих пациентов. Они принимают непосредственное участие в сборе, систематизации, накоплении, хранении, уточнении, обновлении, изменении, распространении и уничтожении такой информации.

Медицинская организация, получая персональные данные от пациента (субъекта персональных данных), например, при его первоначальном поступлении или заключении договора на оказание медицинских услуг, а также в процессе лечения, приобретает статус оператора. У нее возникают определенные обязанности в части работы с полученными персональными данными.

Оператор персональных данных – 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 (ст. 3 Закона № 152-ФЗ).



Основные нормативно-правовые акты

Конституция РФ

Федеральный закон от 27.07.2006 № 152-ФЗ
«О персональных данных»

КоАП РФ,
УК РФ,
ГПК РФ

Федеральный закон
от 27.07.2006 № 149-ФЗ
«Об информации,
информационных
технологиях и о
защите информации»

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

Федеральный закон
от 29.11.2010 № 326-ФЗ
«Об обязательном
медицинском страховании
в российской Федерации»



ПДн пациента и врачебная тайна

ст. 10
152-ФЗ

- информация о состоянии здоровья пациента относится к специальным категориям персональных данных, обработка которых не допускается, за исключением случаев, когда (ст. 10 Закона № 152-ФЗ):
 - пациент дал согласие в письменной форме на обработку своих персональных данных;
 - пациент сам сделал персональные данные общедоступными;

ст. 10
152-ФЗ

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов пациента либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия пациента невозможно;
 - обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну.

ст. 13
323-ФЗ

- Информация, являющаяся врачебной тайной, — это отдельный подвид персональных данных. Она представляет собой сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья, диагнозе и иные сведения, полученные при его медицинском обследовании и лечении (п. 1 ст. 13 Закона № 323-ФЗ). Ее разглашение не допускается (п. 2 ст. 13 Закона № 323-ФЗ), за исключением отдельных случаев, о которых мы расскажем ниже.



Обработка ПДн:

Обработка персональных данных – это любое действие (операция) или совокупность действий (операций), совершаемых с использованием или без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение (ст. 3 Закона № 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. Согласие на обработку персональных данных 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 на дачу согласия от имени субъекта персональных данных проверяются оператором.

Когда СПДн дает согласие в письменной форме





Письменная форма согласия на обработку ПДн

1. Фамилия, имя, отчество, адрес СПДн, номер основного документа, удостоверяющего личность, дата выдачи, орган выдавший документ;
2. Наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
3. Цель обработки персональных данных;
4. Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
5. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
6. Перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
7. Срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
8. Подпись субъекта персональных данных.



Права СПДн на получение информации

СПДн имеет право на получение информации, касающейся обработки его ПДн, в т.ч. содержащей:

подтверждение факта обработки ПДн

правовые основания и цели обработки ПДн

цели способы обработки ПДн

наименование и место нахождения оператора

обрабатываемые ПДн, источник их получения

сроки обработки ПДн и их хранения

порядок осуществления прав СПДн

информация о трансграничной передаче данных

Информация о лице осуществляющем обработку ПДн по поручению оператора

иные сведения предусмотренные 152-ФЗ



Предоставление ПДн третьим лицам:

- ▶ Законодательство запрещает предоставлять третьим лицам и распространять персональные данные без согласия пациента (ст. 7 Закона № 152-ФЗ).
- ▶ Под предоставлением в данном случае понимаются действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц, а под распространением — действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 2 Закона № 152-ФЗ).
- ▶ Вместе с тем, Закон № 323-ФЗ допускает разглашение сведений, составляющих врачебную тайну, с письменного согласия пациента или его законного представителя другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях (п. 2 ст. 13 Закона № 323-ФЗ).
- ▶ Кроме того, предоставление сведений, составляющих врачебную тайну, без согласия пациента или его законного представителя возможно (п. 3 ст. 13 Закона № 323-ФЗ):
 - в целях проведения медицинского обследования и лечения пациента, который в результате своего состояния не способен выразить свою волю;
 - при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;
 - по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля;
 - в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманией либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;
 - в случае оказания медицинской помощи несовершеннолетнему для информирования одного из его родителей или иного законного представителя;
 - в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;
 - в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий;
 - при обмене информацией между медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства РФ о персональных данных;
 - в целях осуществления учета и контроля в системе обязательного социального страхования.

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
КоАП ст. 13.11	Нарушение законодательства Российской Федерации в области персональных данных	
ч. 1	обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи, если эти действия не содержат уголовно наказуемого деяния	влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до трех тысяч рублей; на должностных лиц - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от тридцати тысяч до пятидесяти тысяч рублей
ч. 2	Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством Российской Федерации в области персональных данных, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных	влечет наложение административного штрафа на граждан в размере от трех тысяч до пяти тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от пятнадцати тысяч до семидесяти пяти тысяч рублей

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
КоАП ст. 13.11	Нарушение законодательства Российской Федерации в области персональных данных	
ч. 3	Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных	Влечет предупреждение или наложение административного штрафа на граждан в размере от семисот до одной тысячи пятисот рублей; на должностных лиц - от трех тысяч до шести тысяч рублей; на индивидуальных предпринимателей - от пяти тысяч до десяти тысяч рублей; на юридических лиц - от пятнадцати тысяч до тридцати тысяч рублей
ч. 4	Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных	Влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от четырех тысяч до шести тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до пятнадцати тысяч рублей; на юридических лиц - от двадцати тысяч до сорока тысяч рублей

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
КоАП ст. 13.11	Нарушение законодательства Российской Федерации в области персональных данных	
ч. 5	Невыполнение оператором в сроки, установленные законодательством Российской Федерации в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки,	влечет предупреждение или наложение административного штрафа на граждан в размере от одной тысячи до двух тысяч рублей; на должностных лиц - от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от двадцати пяти тысяч до сорока пяти тысяч рублей
ч. 6	Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния	влечет наложение административного штрафа на граждан в размере от семисот до двух тысяч рублей; на должностных лиц - от четырех тысяч до десяти тысяч рублей; на индивидуальных предпринимателей - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от двадцати пяти тысяч до пятидесяти тысяч рублей

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
КоАП ст. 13.11	Нарушение законодательства Российской Федерации в области персональных данных	
ч. 7	Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных	влечет предупреждение или наложение административного штрафа на должностных лиц в размере от трех тысяч до шести тысяч рублей.

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
УК РФ ч. 1 ст. 137	Незаконное соби́рание или распро́странение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распро́странение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации	наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
УК РФ ч. 2 ст. 137	Незаконное соби́рание 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 с использованием своего служебного положения	наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет

Ответственность за несоблюдение законодательства

Статья	Вид нарушения	Ответственность
УК РФ ст. 140	Неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан	наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет
УК РФ ч. 1 ст. 272	Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети	наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет



СПАСИБО ЗА ВНИМАНИЕ!

Семенов Дмитрий Сергеевич
Заместитель начальника отдела
информационной безопасности ГУЗ «МИАЦ»,
тел. 384-194 доб.11, e-mail:
d.semenenko@mz73.ru

вторник, 3 марта 2020 г.