Утверждаю
Главный врач
К.В. Хомяков
«26» 02 «2021»

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В настоящем Положении используются следующие основные понятия:

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

Обработка персональных данных– действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и

технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1. Общие положения

1.1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных Областного государственного автономного учреждения здравоохранения «Шегарская районная больница»(далее – ОГАУЗ «Шегарская РБ»), от несанкционированного доступа, неправомерного их использования или утраты.

1.2.Настоящее Положение определяет требования к обеспечению безопасности персональных данных в соответствии с законодательством Российской Федерации в области обработки, хранения и защиты персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Настоящее Положение разработано на основании ст. 24 Конституции РФ, Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Постановления Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений.

1.4. Настоящее Положение утверждается Главным врачом ОГАУЗ «Шегарская РБ».

1.5. Изменения в Положение могут быть внесены в установленном действующим законодательством порядке.

2. Понятие и содержание персональных данных

2.1. Оператором персональных данных является ОГАУЗ «Шегарская РБ».

2.3. В ОГАУЗ «Шегарская РБ»осуществляется обработка следующих категорий субъектов персональных данных:

– работники ОГАУЗ «Шегарская РБ»;

– пациенты ОГАУЗ «Шегарская РБ».

3. Порядок получения и обработки персональных данных

3.1 Порядок получения и обработки персональных данных работников ОГАУЗ «Шегарская РБ»

3.1.1. Получение персональных данных работников (а также и кандидатов при приеме на работу)осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых

отношений, защиты персональных данных, нормативными и распорядительными документами ОГАУЗ «Шегарская РБ» на основе согласия субъектов на обработку их персональных данных. При обработке общедоступных персональных данных согласие субъекта не требуется.

3.1.2. Оператор вправе требовать от субъекта персональных данных предоставления информации согласно ст. 6 и ст. 7 Федерального закона № 44 (в том числе о его национальной и расовой принадлежности, состоянии здоровья и др.).

3.1.3. Обработка и использование персональных данных работников в ОГАУЗ «Шегарская РБ» осуществляется в целях реализации кадровой политики ОГАУЗ «Шегарская РБ».

3.1.4. В случае увольнения субъекта персональных данных и иного достижения целей обработки персональных данных, зафиксированных в письменном соглашении, Оператор обязан незамедлительно прекратить обработку персональных данных субъекта и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено Федеральными законами. После увольнения работника документы, содержащие его персональные данные, хранятся в ОГАУЗ «Шегарская РБ» в течение сроков, установленных архивным законодательством.

3.2 Порядок получения и обработки персональных данных пациентов ОГАУЗ «Шегарская РБ»

3.2.1 Получение персональных данных пациентов осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области здравоохранения, защиты персональных данных, нормативными и распорядительными документами ОГАУЗ «Шегарская РБ».

3.2.2 Персональные данные, касающиеся состояния здоровья пациента, относятся к специальным категориям персональных данных и обрабатываются в соответствии с установленным законодательством и иными нормативными правовыми актами требованиями.

3.2.3 Все персональные данные пациента следует получать лично у пациента или у его законного представителя. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. ОГАУЗ «Шегарская РБ»осуществляет обработку персональных данных только после получения письменного согласия пациента (или его

законного представителя) на обработку его персональных данных за исключением случаев, предусмотренных действующим законодательством.

3.2.4 Допускается обработка персональных данных, если она необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно в соответствии с п.6 ст. 6 ФЗ-№152 «О персональных данных».

3.2.5 ОГАУЗ «Шегарская РБ» сообщает пациенту или его законному представителю о целях обработки персональных данных, предполагаемых источниках и способах получения персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

3.2.6 Обработка в ОГАУЗ «Шегарская РБ» персональных данных пациента осуществляется исключительно в целях оказания пациенту качественной медицинской помощи в необходимых объёмах, соблюдения требований действующего законодательства, иных нормативных правовых актов, обеспечения контроля объёмов и качества оказанной медицинской помощи.

4. Порядок использования, хранения, передачи персональных данных ОГАУЗ «Шегарская РБ»

4.1. Персональные данные, обрабатываемые в ОГАУЗ «Шегарская РБ», содержатся в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. Персональные данные могут быть размещены на материальных, в том числе бумажных носителях (медицинская карта пациента, иные медицинские документы – при обработке персональных данных пациентов или карточка Т2, личное дело и иные документы отдела кадров и бухгалтерии – при обработке персональных данных работников).

4.2. Доступ к обработке персональных данных (как с использованием средств автоматизации, так и без использования средств автоматизации) обеспечивается в установленном ОГАУЗ «Шегарская РБ» порядке.

4.3. Конкретные обязанности по работе с информационными системами персональных данных и материальными носителями информации, в том числе с медицинскими документами, содержащими персональные данные пациентов возлагаются на работников ОГАУЗ «Шегарская РБ» и закрепляются в инструкциях.

4.4. Работа с информационными системами персональных данных, материальными носителями, в том числе с медицинской документацией, содержащими персональные данные пациентов осуществляется в специально отведённых для этого помещениях:

– ординаторские, кабинеты врачей, кабинет медицинской статистики, серверная (при обработке персональных данных пациентов);

– кабинет отдела кадров, бухгалтерии, серверная (при обработке персональных данных работников).

4.5. Требования к месту обработки персональных данных, в том числе к серверной, обеспечивающие их защищённость устанавливаются ОГАУЗ «Шегарская РБ» и нормативными документами Российской Федерации в области защиты персональных данных.

4.6. Перечень лиц, имеющих право доступа к персональным данным пациентов и обработке их персональных данных, определяется приказом Главного врача ОГАУЗ «Шегарская РБ».

4.7. С лицами, допущенными к обработке персональных данных пациентов и работников, заключается Соглашение о конфиденциальности.

4.8. Лица, допущенные в установленном порядке к обработке персональных данных, имеют право обрабатывать только те персональные данные, которые необходимы для выполнения конкретных должностных обязанностей.

4.9. ОГАУЗ «Шегарская РБ» при создании и эксплуатации информационных систем персональных данных пациентов с использованием средств автоматизации и без использования средств автоматизации принимает все необходимые организационные и технические меры, обеспечивающих выполнение установленных действующим законодательством требований к обработке персональных данных.

4.10. Передача персональных данных пациента, составляющих врачебную тайну, без согласия пациента или его законного представителя допускается в случаях, предусмотренных ст. 13 Федерального закона от 21.11.2011 N 323-ФЗ (ред. от 30.09.2015) «Об основах охраны здоровья граждан в Российской Федерации» (далее – 323-ФЗ):

1) в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 323-ФЗ;

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов

прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 323-ФЗ, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 323-ФЗ, для информирования одного из его родителей или иного законного представителя;

5) 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;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность;

8) при обмене информацией с медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с 323-ФЗ;

4.11. При передаче персональных данных работники ОГАУЗ «Шегарская РБ» должны соблюдать следующие требования:

– не сообщать персональные данные третьей стороне без письменного согласия субъекта ПДн, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;

– не сообщать персональные данные субъекта ПДн в коммерческих и иных целях без его письменного согласия;

– предупредить лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых

они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности;

– разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом Главного врача, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных должностных функций;

– передавать персональные данные представителям субъекта ПДн в порядке, установленном законодательством, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

5. Права субъектов при обработке ОГАУЗ «Шегарская РБ» персональных данных

5.1. В целях обеспечения защиты своих интересов, реализации прав и свобод в сфере персональных данных, регламентированных действующим законодательством пациенты, их законные представители и работники имеют право на:

– предоставление ОГАУЗ «Шегарская РБ» полной информации об их персональных данных и обработке этих данных;

– свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;

– определение своих представителей для защиты своих персональных данных;

– требование уточнения персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

– требование об извещении ОГАУЗ «Шегарская РБ» всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта ПДн, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжалование действий или бездействия ОГАУЗ «Шегарская РБ» в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Права пациента, представителя, законного представителя, работникана доступ к своим персональным данным ограничиваются в случаях, предусмотренных действующим законодательством.

6. Меры по защите персональных данных, принимаемыев ОГАУЗ «Шегарская РБ»

6.1 Меры по защите персональных данных, принимаемые в ОГАУЗ «Шегарская РБ» носят комплексный характер, а именно, применяютсяследующие категории мер:

– организационные (меры, регламентирующие процессы функционирования информационных систем персональных данных, использование ресурсов информационных систем персональных данных, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с информационными системами персональных данных таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации);

– физические (меры, основанные на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации);

– технические (аппаратно-программные меры защиты, основанные на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое преобразование информации и т.д.)).

Мероприятия по защите персональных данных в ОГАУЗ «Шегарская РБ» являются непрерывными, то есть носят постоянный характер.

6.2 Таким образом, успешное применение технических средств защиты на основании представленных выше принципов предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

– обеспечена физическая целостность всех компонент информационных систем персональных данных;

– каждый работник (пользователь) или группа пользователей информационных систем персональных данных имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

– все изменения конфигурации технических и программных средств информационных систем персональных данных производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства ОГАУЗ «Шегарская РБ»;

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);

– специалистами ОГАУЗ «Шегарская РБ» осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

7. Ответственность за разглашение персональных данных

7.1 Лица, которым в установленном законом порядке переданы сведения, составляющие врачебную тайну, наравне с медицинскими и фармацевтическими работниками с учетом причиненного гражданину ущерба несут за разглашение врачебной тайны дисциплинарную, административную или уголовную ответственность в соответствии с законодательством Российской Федерации, законодательством субъектов Российской Федерации.

7.2 Лица, виновные в нарушении требований законодательства в области защиты персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

7.3 Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

7.4 Работники ОГАУЗ «Шегарская РБ», получившие в установленном порядке доступ к персональным данным пациентов или работников, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных привлекаются к ответственности, предусмотренной действующим законодательством.