

ПОЛОЖЕНИЕ

Об обработке и защите персональных данных в Государственном бюджетном учреждении здравоохранения Республики Карелия «Больница скорой медицинской помощи» (ГБУЗ «БСМП»)

1. Общие положения

1.1. Настоящее Положение определяет порядок получения, учета, обработки, накопления, хранения, передачи и другого использования персональных данных работников и пациентов Государственного бюджетного учреждения здравоохранения Республики Карелия «Больница скорой медицинской помощи» (далее - Оператор, Учреждение).

1.2. Цель настоящего Положения - соблюдение требований законодательства Российской Федерации в области обработки, хранения и защиты персональных данных работников, пациентов и персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации».

1.4. Положение распространяется на отношения по обработке и защите персональных данных, полученных Оператором как до, так и после утверждения настоящего Положения, за исключением случаев, когда по причинам правового, организационного или иного характера Положение не может быть распространено на отношения по обработке и защите персональных данных, полученных до ее утверждения.

1.5. В настоящем Положении используются следующие термины и определения:

Оператор - Государственное бюджетное учреждение здравоохранения Республики Карелия «Больница скорой медицинской помощи»

Субъект - физическое лицо (работник, пациент, иное лицо, состоящее в гражданско-правовых отношениях с Оператором).

Пациент - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от состояния его здоровья.

Медицинская деятельность - профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно - противоэпидемических (профилактических) мероприятий.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку

персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом.

Биометрические персональные данные - сведения, характеризующие физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных.

Использование персональных данных - действия 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.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) - обработка персональных данных, содержащихся в информационной системе персональных данных либо извлечения из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Специальные категории персональных данных - персональные данные, касающиеся расовой и национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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;

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Медицинские данные пациента - сведения о физиологических особенностях организма, перенесенных заболеваниях, состоянии здоровья и (или) оказанной пациенту медицинской помощи.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Третьи лица - лица, не имеющие в установленном порядке допуска к персональным данным.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

2. Персональные данные работника

2.1. В состав персональных данных работников Учреждения входят документы, содержащие сведения о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, а также о предыдущих местах их работы.

2.2. Обработка персональных данных работника осуществляется на основании его письменного согласия, за исключением случаев, прямо предусмотренных действующим законодательством РФ.

2.3 Комплект документов, сопровождающий процесс оформления трудовых отношений работника в Учреждение при его приеме, переводе и увольнении.

2.3.1. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка и (или) сведения о трудовой деятельности (статья 66.1 ТК РФ), за исключением случаев, если трудовой договор заключается впервые;
- документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании и (или) о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН.

2.3.2. При оформлении работника в Учреждение специалистом по кадрам заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие персональные данные работника:

- общие сведения (Ф.И.О. работника, дата рождения, место рождения, пол, гражданство, сведения об образовании (копии документов об образовании), профессия, стаж работы, состояние в браке, наличие /отсутствие смены фамилии, наличие детей, паспортные данные, адрес регистрации и места жительства, номер телефона);
- сведения о воинском учете;
- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:

- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;

- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных льготах;
- сведения о месте жительства и контактных телефонах.

2.3.3. При оформлении работника в Учреждение специалистом по кадрам запрашивается фотография работника с целью оформления пропуска.

2.3.4. В отделе кадров создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

- документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении);
- подлинники и копии приказов по личному составу, содержащие основания к приказу;
- личные карточки по форме Т2 и трудовые книжки работников;
- подлинники и копии отчетных, аналитических и справочных материалов, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

2.4. Работник, как субъект персональных данных, имеет право на получение сведений:

- об операторе, о месте нахождения оператора,
- о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных,
- на подтверждение факта обработки персональных данных оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

2.5. Работник имеет право:

- требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- доступа к своим персональным данным при личном обращении к представителю Учреждения при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

3. Персональные данные пациентов

3.1. В состав персональных данных пациентов Учреждения входят документы, содержащие информацию о паспортных данных, страховом полисе ОМС, ДМС, медицинской карте стационарного, амбулаторного больного (далее медицинские карты), а также иных документах, сопровождающих оказание медицинских услуг.

3.2. Получение персональных данных пациента осуществляется путем представления пациентом письменного согласия на обработку персональных данных, за исключением случаев, прямо предусмотренных действующим законодательством РФ. В случае недееспособности пациента или не достижения пациентом возраста 15 лет согласие на обработку его персональных данных дает в письменной форме его законный представитель.

3.3 Пациент, как субъект персональных данных, в том числе специальной категории персональных данных, имеет право на получение сведений:

- об операторе, о месте нахождения оператора,
- о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных,
- на подтверждение факта обработки персональных данных оператором, а также цели такой обработки;
- о способах обработки персональных данных, применяемые оператором;
- о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- о перечне обрабатываемых персональных данных и источник их получения;
- о сроках обработки персональных данных, в том числе сроки их хранения;
- о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
- на ознакомление с персональными данными, за исключением случая, когда предоставление персональных данных нарушает конституционные права и свободы других лиц.

3.4 Пациент имеет право:

- требовать от оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- доступа к своим персональным данным при личном обращении к представителю Оператора при наличии паспорта;
- доступа к своим персональным данным при направлении письменного запроса, который должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных;
- оформить доверенность на право доступа к его персональным данным;
- принимать предусмотренные законом меры по защите своих прав.

3.5 При поступлении на стационарное или амбулаторное лечение пациент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;
- страховой полис обязательного медицинского страхования (добровольного медицинского страхования);
- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
- иные документы, сопровождающие оказание медицинских услуг.

4. Сбор, обработка и хранение персональных данных

4.1. Все персональные данные субъекта предоставляются им лично путем документального подтверждения.

Если персональные данные субъекта, возможно, получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения

персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

4.2. Учреждение не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами.

Обработка персональных данных, разрешенных для распространения, из числа специальных категорий персональных данных, указанных в ч. 1 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», допускается, если соблюдаются запреты и условия, предусмотренные ст. 10.1 указанного Закона.

4.3. Обработка персональных данных должна осуществляться на основе принципов:

- обработка персональных данных должна осуществляться на законной и справедливой основе;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- 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;

- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

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

4.4. Обработка персональных данных работников Работодателем возможна только с их согласия. Исключение составляют случаи, предусмотренные законодательством Российской Федерации, в частности, согласие не требуется при наличии оснований и соблюдении условий, перечисленных в п. п. 2 - 11 ч. 1 ст. 6, п. п. 2.1 - 10 ч. 2 ст. 10, ч. 2 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в том числе:

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

4.5. Письменное согласие работника на обработку своих персональных данных должно включать в себя, в частности, сведения, указанные в п. п. 1 - 9 ч. 4 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.6. Письменное согласие работника на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. При этом соблюдаются условия, предусмотренные, в частности, ст. 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Требования

к содержанию такого согласия устанавливаются уполномоченным органом по защите прав субъектов персональных данных.

4.6.1. Письменное согласие на обработку персональных данных, разрешенных для распространения, работник предоставляет Работодателю лично.

4.6.2. Работодатель обязан не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.

4.7. Персональные данные субъектов хранятся в электронных базах данных и на бумажных носителях в помещении отдела кадров, бухгалтерии, регистратуре, кабинете статистики, архиве. Для этого используются специально оборудованные шкафы и сейфы. Личные дела уволенных (прошедших обследование, лечение) субъектов хранятся в архиве Учреждения.

4.8. Сведения о начислении и выплате заработной платы работникам Учреждения хранятся в электронных базах данных и на бумажных носителях в помещении расчетной части бухгалтерии. По истечении сроков хранения, установленных законодательством РФ, данные сведения передаются в архив Учреждения.

4.9. Конкретные обязанности по ведению, хранению личных дел субъектов, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные субъектов, возлагается на работников отдела кадров, а по хранению личных дел уволенных (обследованных, пролеченных) субъектов – на работников архива.

4.10. Персональные данные пациентов хранятся в электронных базах данных, а также на бумажных носителях.

4.11. Доступ к электронным базам персональных данных осуществляется в соответствии с утвержденной Политикой безопасности информационных систем персональных данных Учреждения.

4.12. Бумажными носителями персональных данных являются:

- медицинская карта стационарного или амбулаторного больного (медицинская карта), которая заводится на каждого обратившегося в Учреждение за оказанием медицинской помощи при обращении и хранится в Учреждении в сроки, установленные для хранения медицинских карт.

В случае необходимости предоставления медицинской карты в другие подразделения Учреждения для проведения по назначению лечащего врача диагностических исследований, консультаций врачей-специалистов медицинская карта до начала исследования/консультации передается медсестрой отделения медицинскому персоналу соответствующего подразделения, после проведения исследований/консультаций возвращается медицинским персоналом данного подразделения лечащему врачу;

- журналы и другие формы медицинской документации, содержащие персональные данные пациентов, оформляются и хранятся в отделении Учреждения в соответствии с требованиями действующих приказов.

Хранение окончанных производством документов, содержащих персональные данные пациентов, осуществляется в архиве Учреждения.

4.13. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

5. Передача персональных данных субъектов ПД

5.1. При передаче персональных данных субъектов сотрудники Учреждения, имеющие доступ к персональным данным, должны соблюдать следующие требования:

5.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

5.1.2. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

5.1.3. Предупредить лиц, получающих персональные данные субъекта, 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.

5.1.4. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

6. Защита персональных данных.

6.1. Защита персональных данных в Учреждении представляет собой принятие организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации.

6.2. В целях обеспечения безопасности персональных данных при их обработке в информационных системах Учреждения:

- устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- обеспечивается пропускной режим в соответствии с утвержденными документами по охране и осуществлению пропускного режима;
- помещения, в которых ведется работа с персональными данными, оборудуются техническими средствами, обеспечивающими сохранность носителей персональных данных и средств защиты информации, которые исключают возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;
- доступ к информации в электронном виде осуществляется с использованием парольной защиты;
- электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

6.3. Обеспечение безопасности персональных данных в информационных системах персональных данных осуществляется в соответствии с требованиями статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119, нормативными и руководящими документами уполномоченных федеральных органов исполнительной власти.

6.4. Мероприятия по обеспечению безопасности персональных данных проводятся в соответствии с «Составом и содержанием организационным и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

6.5. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых Учреждением угроз безопасности

персональных данных (модели угроз) и в зависимости от уровня защищенности информационной системы, определенного в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012г. №1119.

6.6. Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе системы защиты персональных данных.

6.7. Обеспечение безопасности персональных данных в информационных системах персональных данных без использования средств автоматизации осуществляется в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

6.8. Сотрудники Учреждения, имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников.

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников (пациентов), установленных действующим законодательством, Положением о порядке работы с конфиденциальной информацией и данным Положением, несут дисциплинарную, административную, гражданскую, уголовную или иную ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. Руководители подразделений, в которых происходит обработка персональных данных, несут персональную ответственность за обеспечение защиты обрабатываемых и хранящихся в их подразделениях персональных данных работников (пациентов), посетителей
