

ПОЛОЖЕНИЕ
о защите персональных данных пациентов
ГБУЗ НО «Родильный дом № 5»

Общие положения

1.1. Настоящее Положение определяет порядок получения, учета, обработки, накопления, хранения, передачи и другого использования персональных данных пациентов ГБУЗ НО «Родильный дом №5» (далее - Оператор, Учреждение).

1.2. Цель настоящего Положения - обеспечение организации оказания медицинской помощи, а также 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 N 152-ФЗ «О персональных данных». Федеральным законом от 21.11.2011 N 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 его утверждения.

1.5. В настоящем Положении используются следующие термины и определения:

Оператор – ГБУЗ НО «Родильный дом № 5».

Субъект - физическое лицо (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).

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 извлеченных 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.

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.

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. Состав персональных данных

2.1. Сбор и обработка персональных данных осуществляется исключительно с письменного согласия субъекта. Образцы форм заявлений о согласии на обработку персональных данных и отказа от нее, согласие на медицинское вмешательство и отказ от медицинского вмешательства должны быть утверждены приказами главного врача ГБУЗ НО «Родильный дом 5».

2.1.1. Категории субъектов персональных данных:

- физические лица, обратившиеся в медицинскую организацию за оказанием медицинской помощи.

2.1.2. Оператор осуществляет обработку следующих персональных данных:

- данные, полученные при оказании медицинской помощи.

2.2. В целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных субъекта персональных данных обязаны соблюдать следующие общие требования:

2.2.1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, осуществления медицинской деятельности, и обеспечения сохранности имущества оператора, работника (пациента) и третьих лиц.

2.2.2. Обработка персональных данных может осуществляться для статистических или иных целей при условии обязательного обезличивания персональных данных.

2.2.3. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ, законодательством в области охраны жизни и здоровья граждан и иными федеральными законами.

2.2.4. Информация о персональных данных субъекта предоставляется оператору субъектом устно или письменно. 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 (например, оформление запроса в медицинское учреждение о прохождении

обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

2.2.5. Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и частной жизни.

2.2.6. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.2.7. При принятии решений, затрагивающих интересы субъекта, оператор не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

2.2.8. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством.

2.4. При посещении врача пациент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;
- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
- полис ОМС;
- в отдельных случаях с учетом специфики обследования в учреждение здравоохранения действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

2.5. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, должность, подразделение, служебные телефоны и адрес электронной почты.

2.6. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, областных и муниципальных органов управления. Надзорно - контрольные органы имеют доступ к информации только в пределах своей компетенции.

3. Порядок и условия обработки персональных данных

3.1. Персональные данные субъектов, хранящиеся на бумажных носителях в лечебных отделениях Оператора.

Для этого используются специально оборудованные шкафы и сейфы. Медицинские карты лиц, прошедших обследование и (или) лечение хранятся в архивном хранилище Оператора.

3.2. Конкретные обязанности по ведению, хранению дел субъектов, заполнению, хранению медицинских карт лиц, прошедших обследование и/или лечение иных документов,

отражающих персональные данные субъектов, возлагается на работника делопроизводства, ответственного за архивное делопроизводство и закрепляется в должностной инструкции.

3.4. 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.

Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных, ликвидация или реорганизация Оператора.

3.5. Сведения о субъектах персональных данных Оператора хранятся также на электронных носителях - в базах данных и других регламентированных ИСПДн, согласно перечня ИСПДн, утвержденного приказом главного врача ГБУЗ НО «Родильный дом № 5». Все базы данных находятся на территории Российской Федерации.

3.6. При получении сведений, составляющих персональные данные субъектов заинтересованные лица, имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

3.7. Защита информации о персональных данных.

3.7.1. Сотрудники Оператора, 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.

3.7.2. Оператор при обработке персональных данных предпринимает необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Оператором применяются следующие технические меры по защите информации:

- ограничение сетевого доступа на сервер для определенных пользователей;
- организация в отдельном сегменте сети всех компьютеров пользователей и серверов с ограниченным доступом из локальной сети;
- организация контроля технического состояния серверов и уровней защиты и восстановления информации;
- использование антивирусного программного обеспечения;
- использование ЭП (электронная подпись), СКЗИ (средство криптографической защиты информации).

3.7.3. Защита персональных данных пациентов в Учреждении возлагается на:

- главного врача Учреждения;

- заместителей главного врача;
- работников отдела статистики, операторов;
- руководителей структурных подразделений;
- старших медицинских сестер/акушерок отделений;
- врачей и средний медицинский персонал.

4. Передача персональных данных

4.1. При передаче персональных данных, сотрудники ГБУЗ НО «Родильный дом № 5», имеющие доступ к персональным данным, должны соблюдать следующие требования:

4.1.1. 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. Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта, оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора, отсутствует угроза жизни или здоровью субъекта, оператор обязан отказать в предоставлении персональных данных лицу.

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

4.1.3. 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.

4.1.4. 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.

4.2. Оператор вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

5. Права и обязанности субъектов персональных данных

5.1. Субъект персональных данных вправе требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований законодательства.

5.2. В случае подтверждения факта неточности персональных данных или неправомерности их обработки персональные данные подлежат их актуализации Оператором, а обработка должна быть прекращена, соответственно.

5.3. При достижении целей обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, в срок не позднее 30 календарных дней если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или иными федеральными законами;
- иное не предусмотрено иным соглашением между оператором и субъектом персональных данных.

5.4. Оператор обязан сообщить субъекту персональных данных или его представителю информацию об осуществляемой им обработке персональных данных такого субъекта по запросу последнего.

Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя;
- сведения о дате выдачи указанного документа и органе, его выдавшем;
- подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством РФ.

Срок рассмотрения запроса субъекта персональных данных не может превышать 30 календарных дней с момента его получения медицинской организацией.

5.5. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствующему Субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления Субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) иные сведения, предусмотренные Федеральным законом 152-ФЗ или другими федеральными законами.

5.6. Право Субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с Федеральными законами, в том числе, если доступ Субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

5.7. Ответ в письменной форме на запрос Субъекта должен быть подписан главным врачом Учреждения и отправлен в течение 30 календарных дней в адрес Субъекта через отделение почтовой связи заказным письмом с уведомлением о вручении.

6. Сбор, обработка и хранение персональных данных

6.1. Обработка персональных данных пациентов и работников осуществляется Оператором в части: сбора, записи, уточнения (обновления, изменения), передачи (распространения, предоставления, доступа), обезличивания, извлечения, использования, уничтожения персональных данных.

6.2. Обработка персональных данных пациентов в Учреждении не осуществляется в части систематизации, накопления, хранения, блокирования, удаления персональных данных. Данные виды обработки персональных данных осуществляет организация, выигравшая в соответствии с установленной процедурой сопровождение информационной системы.

6.3. Информацию о персональных данных пациенты Учреждения предоставляют самостоятельно. Федеральными законами 152-ФЗ «О персональных данных», от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и другими федеральными законами предусматриваются случаи обязательного предоставления Субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

7. Доступ к персональным данным Субъекта

7.1. Право доступа к персональным данным Субъектов имеют врачи, средний медицинский персонал и другие должностные лица и работники Учреждения, согласно должностных инструкциям обязанные хранить врачебную и профессиональную тайну.

7.2. Внешний доступ.

К числу массовых потребителей персональных данных вне Учреждения относятся государственные и негосударственные структуры: правоохранительные органы; органы прокуратуры и ФСБ; военкоматы; органы социального страхования; пенсионные фонды; вышестоящие организации; центры обработки данных. Согласно действующему законодательству Российской Федерации.

7.3. Родственники и члены семей.

Персональные данные субъекта могут быть предоставлены только его законному представителю с письменного разрешения самого субъекта.

8. Защита персональных данных Субъекта

8.1. В целях обеспечения сохранности и конфиденциальности персональных данных Субъектов все операции по обработке, ведению и хранению

данной информации должны выполняться только должностными лицами, обязанными хранить врачебную и профессиональную тайну в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

8.2. Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и представленных полномочий даются в письменной форме с исходящим номером на бланке Учреждения и в том объеме, который позволяет не разглашать излишний объем персональных сведений о пациентах и работниках.

9. Ответственность за разглашение информации, связанной с персональными данными

В соответствии со ст. 13 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» 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.

Не допускается разглашение сведений, составляющих врачебную тайну лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме оговоренных законом случаев.

Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается только в случаях, предусмотренным законодательством.

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.

Согласно ст. 24 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований, несут предусмотренную законодательством Российской Федерации ответственность.

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