УТВЕРЖДАЮ

Главный врач

 Комарова Т.А.

БУЗ ВО “Бабушкинская ЦРБ”

**ПОЛОЖЕНИЕ**

по обработке и защите персональных пациентов и их законных представителей
БУЗ ВО «Бабушкинская ЦРБ»
с. Бабушкино
2022 г.

1. Общие положения
	1. Целью данного Положения является защита персональных данных пациентов от несанкционированного доступа, неправомерного их использования или утраты.
	2. Настоящим Положением определяется порядок обработки персональных данных пациентов БУЗ ВО «Бабушкинская ЦРБ».
	3. Обработка персональных данных пациентов осуществляется в целях обеспечения соблюдения законов, исполнения нормативно-правовых актов, регулирующих медицинскую и иную деятельность организации, содействия пациентам в предоставлении услуг, контроля количества и качества выполняемой работы и обеспечения сохранности имущества. А гак же обеспечения безопасности пребывания на территории учреждения пациентов и их законных представителей. Предоставления медицинских, других лицензируемых услуг.
	4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 25 лет срока хранения, если иное не определено законом.
	5. Настоящее Положение утверждается и вводится в действие приказом Главного врача и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.
2. Основные понятия. Состав персональных данных
	1. Для целей настоящего Положения используются следующие основные понятия:
		1. персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		2. 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 Федеральным законом от 27.07.2006 N 152-ФЗ (далее - персональные данные, разрешенные для распространения) (п. 1.1. ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		3. оператор - 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 (п. 2 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		4. обработка персональных данных пациента - 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 (п, 3 ст. 3 Федерального закона от 27,07,2006 N 152-ФЗ);
		5. распространение персональных данных - действия, направленные на раскрытие персональных данных пациентов неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		6. передача персональных данных - действия, направленные на раскрытие персональных данных пациентов определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		7. блокирование персональных данных - временное прекращение обработки персональных данных пациентов (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		8. уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных пациентов и (или) в результате которых уничтожаются материальные носители персональных данных пациентов (п. 8 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);
		9. обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному пациенту (п. 9 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ).
	2. В состав персональных данных пациентов входит:
* паспортные данные;
* адрес;
* данные свидетельства о рождении;
* страховой помер индивидуального лицевого счета;
* данные об образовании и профессии;
* данные о детях;
* данные о семейном положении;
* данные полиса ОМС;
* сведения о профилактических прививках;
* социальное положение;
* состояние здоровья;
* пол;
* образование;
* профессия.
	1. Все документы, содержащие персональные данные пациентов, являются конфиденциальными, но, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.
1. Обработка персональных данных
	1. Источником информации обо всех персональных данных пациента является непосредственно пациент. Получение персональных данных может осуществляться как путем представления их самим пациентом или его законным представителем, так и путем получения их из иных источников.
	2. Если персональные данные возможно получить только у третьей стороны, то пациент должен быть заранее в письменной форме уведомлен об этом и от пего или законным его представи телем должно быть получено письменное согласие за исключением случаев, предусмотренных федеральными и территориальными законами. БУЗ ВО «Бабушкинская ЦРБ» обязано сообщить пациенту или его законному представителю о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента или его законного представителя дать письменное согласие па их получение.
	3. БУЗ ВО «Бабушкинская ЦРБ» по имеет права получать и обрабатывать персональные данные пациента или его законного представителя о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, интимной жизни, за исключением случаев, предусмотренных в ч. 2 и 2.1 ст. 10 Федерального закона от 27.07.2006 N 152-ФЗ.
		1. Обработка персональных данных, разрешенных для распространения, из числа специальных категорий персональных данных, указанных в ч. 1 ст. 10 Федерального закона от 27.07.2006 N 152-ФЗ, допускается, если соблюдаются запреты и условия, предусмотренные ст. 10,1 указанного Закона.
	4. БУЗ ВО «Бабушкинская ЦРБ» не имеет права получать и обрабатывать персональные данные пациентов или его законного представителя о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законам и.
	5. Обработка персональных данных пациентов в БУЗ ВО «Бабушкинская ЦРБ» возможна только с их согласия или согласия их законных представителей. Исключение составляют случаи, предусмотренные законодательством РФ (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 N 152-ФЗ).
	6. Письменное согласие пациента или его законного представителя 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 N 152-ФЗ.
	7. Письменное согласие пациента или его законного представителя 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 N 152-ФЗ. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 N 18.
		1. Письменное согласие на обработку персональных данных, разрешенных для распространения, пациент или его законный представитель предоставляет в БУЗ ВО «Бабушкинская ЦРБ» лично.
		2. Согласие на обработку персональных данных, разрешенных для распространения, прекращает свое действие с момента поступления в БУЗ ВО «Бабушкинская ЦРБ» требования, указанного в 9.1.7. настоящего Положения.
	8. Пациент или его законный представитель в БУЗ ВО «Бабушкинская ЦРБ» обязан представлять достоверные сведения. Сотрудники БУЗ ВО «Бабушкинская ЦРБ», получившие данные пациентов, обязаны по возможности осуществлять проверку достоверности сведений и уточнение.
	9. При определении объема и содержания, обрабатываемых персональных данных пациента и его законного представителя, БУЗ ВО «Бабушкинская ЦРБ» должна руководствоваться Конституцией РФ и иными федеральными законами.
	10. При принятии решений, затрагивающих интересы пациента, БУЗ ВО «ВОДКБ нс имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки.
2. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
3. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации па основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
4. Передача персональных данных
	1. Передача персональных данных пациента возможна только с согласия пациента или его законного представителя, или в случаях, прямо предусмотренных законодательством. При передаче персональных данных пациентов в БУЗ ВО «Бабушкинская ЦРБ» должны соблюдать следующие требования:
		1. Не сообщать персональные данные пациента третьей стороне без письменного согласия пациента или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральными законами,
		2. Не сообщать персональные данные пациента в коммерческих целях без его письменного согласия.
		3. Осуществлять передачу персональных данных пациентов в пределах БУЗ ВО «Бабушкинская ЦРБ» в соответствии с настоящим Положением.
		4. Предупредить ответственных лиц, получающих персональные данные пациента, о

том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные пациента, обязаны соблюдать режим секретности

(конфиденциальности) и требования настоящего положения. Данное правило нс

распространяется на обмен персональными данными пациентов в порядке, установленном федеральными законами.

* + 1. Передавать персональные данные пациента представителям пациентов в порядке, установленном федеральными законами, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями заявленных целей предоставления.
	1. Не допускается передавать персональные данные по телефону или факсу, в том числе давать отве ты, содержащие персональные данные.
	2. Нс допускается передача персональных данных по открытым каналам связи, в том числе не сертифицированным ФСТЭК РФ (электронная почта и т.д.).
1. Храпение персональных данных
	1. Персональные данные пациентов на бумажных носителях хранятся исключительно на территории БУЗ ВО «Бабушкинская ЦРБ»,
	2. Персональные данные пациентов в электронном виде хранятся в 11.ОД БУЗ ВО «Бабушкинская ЦРБ» и ЦОД организаций, ответственных за предоставление доступа к информационным системам, в которых обрабатываются персональные данные пациентов.
	3. Храпение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.
	4. В БУЗ ВО «Бабушкинская ЦРБ» персональные данные хранятся в специально отведенных системах хранения: шкафах, сейфах, либо в запираемых помещениях, с ограниченным правом доступа.
	5. Ключи от мест храпения хранятся у ответственных лиц.
	6. Персональные данные пациентов БУЗ ВО «Бабушкинская ЦРБ» в электронном виде хранятся в информационных системах персональных данных больницы (серверах), в электронных папках и файлах в ПК работников больницы, ЦОД БУЗ ВО «Бабушкинская ЦРБ» и ЦОД организаций, ответственных за предоставление доступа к информационным системам.
	7. Хранение персональных данных пациентов осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению но их достижении или в случае утраты необходимости в их достижении при этом срок хранения персональных данных должен быть не ниже срока установленного законодательством РФ.
	8. Персональные данные, содержащиеся па бумажных носителях, сдаются в архив на хранение после окончания сроков их обработки.
2. Уточнение, блокирование и уничтожение персональных данных
	1. Уточнение персональных данных, в том числе их обновление и изменение, имеет своей целью обеспечение достоверности, полноты и актуальности персональных данных, обрабатываемых ЛПУ.
	2. Уточнение персональных данных осуществляется ЛПУ по собственной инициативе, по требованию субъекта персональных данных или его законного представителя, по требованию уполномоченного органа по защите прав субъектов персональных данных в случае, когда установлено, что персональные данные являются неполными, устаревшими, недостоверными, в других случаях предусмотренных в нормативных актах РФ.
	3. Блокирование персональных данных осуществляется ЛПУ по требованию субъекта персональных данных или его законного представителя, а также по требованию уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними. О блокировании персональных данных ЛПУ обязано уведомить субъект персональных данных или его законного представителя.
	4. Уничтожение персональных данных, за исключением случаев необходимости обработки персональных данных, предусмотренных законодательством, осуществляется:
* по достижении цели обработки персональных данных;
* в случае утраты необходимости в достижении целей обработки персональных данных;
* по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных в случаях, определенных в законодательстве РФ.

6.5.13 целях обеспечения законности при обработке персональных данных и устранения факторов, влекущих или могущих повлечь неправомерные действия с персональными данными, ЛПУ вправе по собственной инициативе осуществить блокирование и (или) уничтожение персональных данных.

О блокировании и (или) уничтожении персональных данных ЛПУ обязано уведомить субъекта персональных данных или его законного представителя.

1. Персональные данные уничтожаются ио акту по истечению установленного срока хранения, указанного в настоящем положении.
2. Уничтожение документов, содержащих персональные данные пациентов, производиться путем дробления (измельчения), превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера с классом секретности нс ниже 5.
3. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителей, без возможности восстановления удаленных данных.
4. Доступ к персональным данным
	1. Внутренний доступ (доступ внутри организации).

7.1.1 Право доступа к персональным данным пациентов имеют:

* главный врач;
* руководители и работники медицинских структурных подразделений по направлению деятельности;
* другие работники организации при выполнении ими своих должностных обязанностей.
	1. Внешний доступ.
		1. Структуры, для которых возможна передача персональных данных пациентов, осуществляется в соответствии ч. 4 ст, 13 Федерального закона от 21.11.2011 г. № 323-ФЗ.
		2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
		3. Сведения о пациенте могут быть предоставлены в ответ на письменный запрос, оформленный па бланке организации, заверенный подписью руководителя организации и печатью, с приложением копии заявления пациента или его законного представи теля.
		4. Персональные данные пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента или его законного представителя.
1. Защита персональных данных
	1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.
	2. Риск угрозы персональных данных пациентов создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоя тельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.
	3. Защита персональных данных представляет собой регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации.
	4. Защита персональных данных пациента от неправомерного использования или утраты должна быть обеспечена БУЗ ВО «Бабушкинская ЦРБ» за счет собственных средств, в порядке, установленном федеральным законом.
	5. Внутренняя защита персональных данных,
		1. Для обеспечения внутренней защиты персональных данных пациентов необходимо соблюдать ряд мер:
* регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных;
* ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным пациентов;
* строго избирательное и обоснованное распределение информации между работниками;
* рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
* знание работником требований нормативно - методических документов по защите информации и сохранении тайны, в соответствии с требованиями настоящего положения;
* наличие необходимых условий в помещении для работы с персональными данными пациентов и базами данных;
* определение и регламентация состава работников, имеющих право доступа в помещения, в которых хранятся персональные данные пациентов;
* организация порядка уничтожения информации;
* своевременное выявление нарушений требований контроля доступа работниками подразделения;
* воспитательная и разъяснительная работа с работниками подразделений по предупреждению утраты ценных сведений при работе с персональными данными пациентов;
* медицинские карты амбулаторного больного могут выдаваться па рабочие места только врачу, ведущему прием конкретного пациента, в других случаях но согласованию с главным врачом - руководителям структурных подразделений (например, при подготовке материалов для ответа на обращение и жалобу).
* медицинские карты стационарного больного доступны медицинскому персоналу больницы, участвующему в лечении конкретного пациента, в других случаях по согласованию с главным врачом - руководителям структурных подразделений (например, при подготовке материалов для ответа на обращение и жалобу).
	+ 1. Защита персональных данных пациентов на электронных носителях.

Доступ ко всем панкам, содержащих персональные данные, должны быть строго регламентированы в соответствии с распоряжением главного врача № 11 от 06.10.2022г.

* 1. Внешняя защита персональных данных.
		1. Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией, технические и организационные средства защиты.
		2. Под посторонним лицом понимается любое лицо, по имеющее непосредственного отношения к деятельности организации, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и храпения документов, дел и рабочих материалов.
		3. Для обеспечения внешней защиты персональных данных пациентов необходимо соблюдать ряд мер:
* пропускной режим учреждения;
* технические средства охраны, сигнализации - поддержка в исправном состоянии;
* порядок охраны территории, зданий, помещений, транспортных средств;
* требования к защите информации при обработке в информационных системах БУЗ ВО «Бабушкинская ЦРБ»;

-использовать сертифицированные ФСТЭК средства защиты информации при передаче персональных данных пациентов.

* 1. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных пациентов.
	2. По возможности персональные данные обезличиваются.
1. Права и обязанности
	1. 13 целях защиты персональных данных, хранящихся в организации, пациент и законный его представитель имеет право:
		1. требовать исключения или исправления неверных или неполных персональных данных.
		2. па свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
		3. персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
		4. определять своих представителей для получения своих персональных данных;
		5. на сохранение и защиту своей личной и семейной тайпы;
		6. получать от БУЗ ВС) «Бабушкинская ЦРБ» сведения о наименовании и месте 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 (по письменному запросу).
		7. требовать прекратить в любое время передачу (распространение, предоставление, доступ) персональных данных, разрешенных для распространения. Требование оформляется в письменном виде. Оно должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) работника, а также перечень персональных данных, обработка которых подлежит прекращению, за исключением случаев, предусмотренных законодательством.
	2. Пациент или его законный представитель обязан своевременно сообщать об изменении своих персональных данных, в частности об изменении фамилии, имени, отчества, даты рождения. Так же сообщаются данные о полисе, адресе, СНИЛС.
2. Ответственность за разглашение конфиденциальной информации, связанной с
персональными данными
	1. Ответственные лица, в соответствии со своими полномочиями владеющие информацией о пациентах, получающие и использующие ее, несут персональную ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
3. Руководитель структурного подразделения, разрешающий доступ работника к персональным данным пациента для выполнения возложенных обязанностей, несет персональную ответственность за соблюдение таким работником требований настоящего Положения.
4. Каждый работник организации, получающий для работы персональные данные пациента, несет, в том числе персональную ответственность за сохранность носителя и персональных данных пациента.
5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
6. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.
7. В соответствии с Гражданским Кодексом лица, незаконными методами получившие конфиденциальную информацию, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и па работников.
8. Уголовная ответственность за нарушение неприкосновенности частной жизни ( в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.
9. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.
10. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных пациента, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном ф ед ер ал ь н ы м и за к о и а м и.
11. Моральный вред, причиненный пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 N 152- ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных пациентом убытков.
12. Заключительные положения
13. Настоящее Положение вступает в силу с момента его утверждения главным врачом Л ПУ и действует бессрочно, до замены его новым Положением.
14. При необходимости приведения настоящего Положения в соответствии с вновь принятыми законодательными актами, изменения вносятся на основании Приказа главного врача БУЗ ВО «Бабушкинская ЦРБ».
15. Настоящее Положение действует в отношении всех пациентов или их законных представителей, а также работников БУЗ ВО «Бабушкинская ЦРБ», имеющих доступ и осуществляющих перечень действий с персональными данными пациента.
16. В обязанности работников, осуществляющих первичный сбор персональных данных пациента или его законного представителя, входит получение согласия пациента или его законного представителя на обработку персональных данных под личную подпись.