

Бюджетное учреждение здравоохранения
Удмуртской Республики
«Кезская районная больница Министерства здравоохранения
Удмуртской Республики»

ПРИКАЗ

22 февраля 2017 г.

№ 93

г. Ижевск

**«Об утверждении Политики в
отношении обработки и защиты
персональных данных»**

Во исполнение требований, предусмотренных п.2 ч.1 ст. 18.1 и ч.2 ст. 18.1
Федерального закона РФ «О персональных данных» № 152-ФЗ от 27 июля 2006 года,

ПРИКАЗЫВАЮ:

1. Утвердить Политику обработки и защиты персональных данных (Приложение № 1).
2. Начальнику отдела правовой работы Гаврилову А.Ю. до «28» февраля 2017 года опубликовать на сайте БУЗ УР «Кезская РБ МЗ УР» Политику в отношении обработки и защиты персональных данных.
3. Контроль над исполнением оставляю за собой.

Главный врач БУЗ УР «Кезская РБ МЗ УР»



Л.А. Малыгин

Утверждено
Приказом главного врача
БУЗ УР «Кезская РБ МЗ УР»
от «22» февраля 2017 г. № 93

**Политика
обработки и защиты персональных данных
БУЗ УР «Кезская РБ МЗ УР»**

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона РФ «О персональных данных» №152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных (далее – ПДн), которые Бюджетное учреждение здравоохранения Удмуртской Республики «Кезская районная больница Министерства здравоохранения Удмуртской Республики» (далее – БУЗ УР «Кезская РБ МЗ УР») может получить от субъекта персональных данных, являющегося стороной по гражданско-правовому договору, а так же от субъекта персональных данных, состоящего с БУЗ УР «Кезская РБ МЗ УР» в отношениях, регулируемых трудовым законодательством (далее – Работника).

1.2. БУЗ УР «Кезская РБ МЗ УР» обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», локальных нормативных актов БУЗ УР «Кезская РБ МЗ УР».

1.3.Изменение Политики :

1.3.1. БУЗ УР «Кезская РБ МЗ УР» имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте организации, если иное не предусмотрено новой редакцией Политики.

1.3.2. Действующая редакция хранится в месте нахождения исполнительного органа БУЗ УР «Кезская РБ МЗ УР» по адресу: 427580, УР, Кезский район, п. Кез, ул.Больничный городок, д.1, электронная версия Политики на сайте БУЗ УР «Кезская РБ МЗ УР» по электронному адресу:

2. Термины и принятые сокращения

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

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.

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.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Информационная система персональных данных (ИСПДн) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

3. Обработка персональных данных

3.1. Получение персональных данных:

3.1.1. Все персональные данные следует получать от самого субъекта. Если персональные данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

3.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональными данными, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

3.1.3. Документы, содержащие персональные данные создаются путем:

- а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- б) внесения сведений в учетные формы;
- в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.)

3.2. Обработка персональных данных:

3.2.1 Обработка персональных данных осуществляется:

- согласия субъекта персональных данных на обработку его персональных данных;
- в случаях, когда обработка персональных данных необходима для осуществления и выполнения, возложенных законодательством Российской Федерации функций, полномочий и обязанностей;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

3.2.2 Цели обработки персональных данных:

- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

3.2.3 Категории субъектов персональных данных.

В БУЗ УР «Кезская РБ МЗ УР» обрабатываются персональные данные следующих субъектов ПДн:

- физические лица, состоящие с БУЗ УР «Кезская РБ МЗ УР» в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников БУЗ УР «Кезская РБ МЗ УР»;
- физические лица, уволившиеся из БУЗ УР «Кезская РБ МЗ УР»;
- пациенты находящиеся на обслуживании БУЗ УР «Кезская РБ МЗ УР»;
- физические лица, состоящие с БУЗ УР «Кезская РБ МЗ УР» в гражданско-правовых отношениях.

3.2.4 Персональные данные, обрабатываемые в БУЗ УР «Кезская РБ МЗ УР»:

- персональные данные, полученные при осуществлении трудовых отношений;
- персональные данные, полученные от пациентов БУЗ УР «Кезская РБ МЗ УР»;

- персональные данные, полученные при осуществлении гражданско-правовых отношений.

Полный список персональных данных представлен в Перечне персональных данных, утвержденном главным врачом БУЗ УР «Кезская РБ МЗ УР».

3.2.5 Обработка персональных данных ведется:

- с использованием средств автоматизации;
- без использования средств автоматизации.

3.3.Хранение персональных данных:

3.3.1. Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде.

3.3.2. Персональные данные, зафиксированные на бумажных носителях хранятся в запираемых шкафах.

3.3.3. Персональные данные субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (хранилищах).

3.3.4. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в информационной системе персональных данных.

3.3.5. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.4.Уничтожение персональных данных:

3.4.1. Уничтожение документов (носителей), содержащих персональные данные производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

3.4.2. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

3.4.3 Уничтожение производится комиссией. Факт уничтожения персональных данных подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

3.5.Передача персональных данных:

3.5.1. БУЗ УР «Кезская РБ МЗ УР» передает персональные данные третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским законодательством в рамках установленной законодательством процедуры.

3.5.2. Перечень лиц (организаций), которым передаются персональные данные:

- пенсионный фонд РФ для учета (на законных основаниях);
- налоговые органы РФ (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- бюро кредитных историй (с согласия субъекта);
- юридические и коллекторские фирмы, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

4. Защита персональных данных

4.1. В соответствии с требованиями нормативных документов в БУЗ УР «Кезская РБ МЗ УР» создана система защиты персональных данных (далее - СЗИ/Дн), состоящая из подсистем правовой, организационной и технической защиты.

4.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗИ/Дн.

4.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗИ/Дн, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

4.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

4.5. Основными мерами защиты персональных данных, используемыми БУЗ УР «Кезская РБ МЗ УР», являются:

4.5.1. Назначение лица, ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением БУЗ УР «Кезская РБ МЗ УР» и его работниками требований к защите персональных данных, организует прием и обработку обращений и запросов субъектов персональных и третьих лиц.

4.5.2. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, и разработка мер и мероприятий по защите персональных данных.

4.5.3. Разработка политики в отношении обработки персональных данных, реализуемых требований к защите персональных данных.

4.5.4. Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных.

4.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

4.5.6. Применение прописанных в установленном порядке процедуры оценки соответствия средств защиты информации.

4.5.7. Применение сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами.

4.5.8. Применение сертифицированных программных средств защиты информации от несанкционированного доступа.

4.5.9. Установлены: сертифицированный межсетевой экран и средства обнаружения вторжения.

4.5.10. Обмен персональными данными при их обработке в информационных системах персональных данных осуществляется по защищенным каналам связи.

4.5.11. Соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

4.5.12. Организован учет материальных носителей персональных данных.

4.5.13. Осуществляется обнаружение фактов несанкционированного доступа к персональным данным с принятием мер.

4.5.14. Осуществляется восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.5.15. Проводится обучение работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику БУЗ УР «Кезская РБ МЗ УР», в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

4.5.16. Осуществляется внутренний контроль и аудит безопасности персональных данных при их обработке в информационных системах персональных данных..

5. Основные права субъекта персональных данных и обязанности оператора

5.1. Основные права субъекта персональных данных:

Субъект имеет право на:

- доступ к его персональным данным;
- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- 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;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральными законами;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- обращения к оператору и направление ему запросов;
- обжалование действий или бездействия оператора.

5.2. Обязанности Оператора:

- при сборе персональных данных предоставить информацию об обработке его персональных данных;
- в случаях если персональные данные были получены не от субъекта персональных данных уведомить субъекта;
- при отказе в предоставлении персональных данных субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу,

определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных;

- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

- давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.