



**Бюджетное учреждение здравоохранения Удмуртской Республики
«Сарапульская районная больница Министерства здравоохранения
Удмуртской Республики»**

ПРИКАЗ

«21» июля 2016 года

№ 151/5

«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. Заместителю главного врача по кадрам Гайсиной Г.Д. до «15» августа 2016 года опубликовать на сайте БУЗ УР «Сарапульская РБ МЗ УР» Политику в отношении обработки и защиты персональных данных.
3. Контроль над исполнением оставляю за собой.

Главный врач БУЗ УР «Сарапульская РБ МЗ УР» 

И.Н. Шихова

Приложение № 1

Утверждено
Приказом главного врача
БУЗ УР «Сарапульская РБ МЗ УР»
от «01» июля 2016 г. № 151/5

Политика обработки и защиты персональных данных БУЗ УР «Сарапульская 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 «Сарапульская районная больница Министерства здравоохранения Удмуртской Республики» (далее – БУЗ УР «Сарапульская 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 «Сарапульская РБ МЗ УР» в отношениях, регулируемых трудовым законодательством (далее – Работника).

1.2. БУЗ УР «Сарапульская 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 «Сарапульская РБ МЗ УР».

1.3. Изменение Политики.

1.3.1. БУЗ УР «Сарапульская 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 «Сарапульская РБ МЗ УР» по адресу: Удмуртская Республика, 427990, УР, Сарапульский район, с. Сигаево, ул. Советская, д. 110, электронная версия Политики – на сайте БУЗ УР «Сарапульская РБ МЗ УР» по электронному

адресу: www//srbol.ru//

2. Термины и принятые сокращения

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

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;

Персональные данные, сделанные общедоступными субъектом персональных данных - ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

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;

3. Обработка персональных данных

3.1. Получение ПДн:

3.1.1. Все ПДн следует получать от самого субъекта. Если ПДн 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 ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, 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 ПДн 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 ПДн:

3.2.1 Обработка персональных данных осуществляется:

- С 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 «Сарапульская РБ МЗ УР» обрабатываются ПДн следующих субъектов ПДн:

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

3.2.4 ПДн, обрабатываемые БУЗ УР «Сарапульская РБ МЗ УР»:

- ПДн, полученные при осуществлении трудовых отношений;
- ПДн, полученные при осуществлении учебного процесса от студентов;
- ПДн, полученные при осуществлении гражданско-правовых отношений.

Полный список ПДн представлен в Перечне ПДн, утвержденном главным врачом БУЗ УР «Сарапульская РБ МЗ УР»

3.2.5 Обработка персональных данных ведется:

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

3.3. Хранение ПДн

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

3.3.2. ПДн, зафиксированные на бумажных носителях хранятся в запираемых шкафах.

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

3.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПДн.

3.3.5. Хранение ПДн в форме, позволяющей определить субъекта ПДн, 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 ПДн

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

3.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

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

3.5. Передача ПДн

3.5.1. БУЗ УР «Сарапульская РБ МЗ УР» передает ПДн 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, которым передаются ПДн

- 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 «Сарапульская РБ МЗ УР» создана система защиты персональных данных (СЗПДн), 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 СЗПДн.

4.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПДн, 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 ПДн.

4.5. Основными мерами защиты ПДн, используемыми БУЗ УР «Сарапульская РБ МЗ УР», являются:

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

4.5.2 Определение актуальных угроз безопасности ПДн при их обработке в ИСПДн, и разработка мер и мероприятий по защите ПДн;

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

4.5.4 Установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;

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

4.5.6 Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4.5.7 Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

4.5.8 Сертифицированное программное средство защиты информации от несанкционированного доступа;

4.5.9 Сертифицированные межсетевой экран и средство обнаружения вторжения;

4.5.10 Обмен ПДн при их обработке в ИСПДн осуществляется по защищенным каналам связи;

4.5.11. Соблюдаются условия, обеспечивающие сохранность ПДн и исключают

несанкционированный к ним доступ.

4.5.12 Организация учета машинных носителей персональных данных;

4.5.13 Обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

4.5.14 Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.5.15 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 «Сарапульская РБ МЗ УР», в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

4.5.16 Осуществление внутреннего контроля и аудита.

5. Основные права субъекта ПДн и обязанности оператора

5.1. Основные права субъекта ПДн

Субъект имеет право на:

- доступ к его персональным данным и следующим сведениям:
 - подтверждение факта обработки ПДн оператором;
 - правовые основания и цели обработки ПДн;
 - цели и применяемые оператором способы обработки ПДн;
 - наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
 - сроки обработки персональных данных, в том числе сроки их хранения;
 - порядок осуществления субъектом ПДн прав, предусмотренных настоящим Федеральным законом;
 - наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн 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 ПДн предоставить информацию об обработке его ПДн;
- В случаях если ПДн были получены не от субъекта ПДн уведомить субъекта;
- При отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн;
- Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД а также от иных неправомерных действий в отношении ПДн;
- Давать ответы на запросы и обращения Субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

Заместитель главного врача по кадрам

Г.Д. Гайсина