

**1. Общие положения.**

1.1. Настоящий документ определяет политику бюджетного учреждения здравоохранения Воронежской области «Воронежский областной клинический центр профилактики и борьбы со СПИД» (далее - Оператор) в отношении обработки персональных данных (далее - ПДн).

1.2. Настоящая политика в области обработки и защиты ПДн (далее - Политика) разработана в соответствии с п. 2 ст. 18.1 Федерального закона «О персональных данных» №152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных, обрабатываемых Оператором.

1.3. Целью настоящей Политики является защита интересов Оператора, его работников, субъектов ПДн. обрабатываемых Оператором, а также выполнение законодательства Российской Федерации о персональных данных.

1.4. Политика распространяется на Данные, полученные как до, так и после подписания настоящей политики.

1.5. В целях гарантированного выполнения норм федерального законодательства Оператор считает важнейшей задачей соблюдение принципов законности, целостности и конфиденциальности при обработке ПДн, а также обеспечение безопасности процессов их обработки.

1.6. Политика характеризуется следующими признаками:

1.6.1. Разработана в целях обеспечения реализации требований законодательства РФ в области обработки ПДн субъектов персональных данных.

1.6.2. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором ПДн, права и обязанности оператора при обработке ПДн, права субъектов ПДн, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности ПДн при их обработке.

1.6.3. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке ПДн.

1.7. Действие настоящего документа распространяется на все процессы, в рамках которых осуществляется обработка персональных данных субъектов ПДн всех категорий, а также на подразделения, принимающие участие в указанных процессах.

1.8. Основные положения документа могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействие с Оператором в качестве поставщиков и потребителей (пользователей) информации.

1.9. Правовой основой настоящего документа является Федеральный закон №152-ФЗ «О персональных данных» от 27 июля 2006 года.

**2. Термины и определения.**

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

2.2. Оператор – Учреждение, осуществляющее обработку персональных данных.

2.3. 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.

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

**3. Информация об Операторе.**

Наименование: бюджетное учреждение здравоохранения Воронежской области «Воронежский областной клинический центр профилактики и борьбы со СПИД»

ИНН: 3662044189

Фактический адрес: 394065, г. Воронеж, пр-т Патриотов, 29б

Телефон/Факс (473) 270-51-16

E-mail: [postmaster@aidsvrn.ru](mailto:postmaster@aidsvrn.ru)

Сайт в сети Интернет: <http://voronezh-aids.ru/>

Сайт на портале департамента здравоохранения Воронежской области: http://vocpbs.medportal.oblzdrav.vrn.ru/

Регистрационный номер записи в Реестре операторов, осуществляющих обработку персональных данных: 10-0153559. Страница на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций: http://pd.rkn.gov.ru/operators-registry/operators-list/?id=10-0153559.

**4. Правовые основания обработки персональных данных.**

4.1. Политика Оператора в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами РФ:

4.1.1. Конституция Российской Федерации.

4.1.2. Трудовой кодекс Российской Федерации.

4.1.3. Гражданский кодекс Российской Федерации.

4.1.4. Федеральный закон от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

4.1.5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

4.1.6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

4.1.7. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.1.8. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при из обработке в информационных системах персональных данных (ФСБ России. №149/6/6-622, 2008).

4.1.9. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждено приказом директора ФСТЭК России от 18.02.2013 N 21).

4.1.10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена 14.02.2008 заместителем директора ФСТЭК России).

4.1.11. Федеральный закон от 21.11.2011 №323-Ф3 "Об основах охраны здоровья граждан в Российской Федерации".

4.1.12. Федеральный закон от 29.11.2010 № 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации"

4.2. Во исполнение настоящей Политики Оператором утверждены следующие локальные нормативные правовые акты:

4.2.1. Положение об обработке ПДн.

4.2.2. Положение об обеспечении безопасности ПДн.

4.2.3. Перечень информационных систем персональных данных.

4.2.4. Перечень ПДн, обрабатываемых в информационных системах персональных данных.

4.2.5. Приказ об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

4.2.6. Акт классификации информационной системы персональных данных.

4.2.7. Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных.

4.2.8. Приказ об утверждении списка лиц, которым необходим доступ к ПДн, обрабатываемым в информационных системах персональных данных, для выполнения служебных (трудовых) обязанностей (и соответствующие приказы по дополнению списка).

4.2.9. Инструкции пользователей информационных систем персональных данных.

**5. Цели обработки персональных данных.**

5.1. Оператор, как медицинская организация, оказывающая высококвалифицированную специализированную консультативно - диагностическую и лечебную медицинскую помощь гражданам Российской Федерации на территории Воронежской области в амбулаторных и стационарных условиях с применением высокоэффективных медицинских технологий, обрабатывает персональные данные исключительно в следующих целях, согласно реестру операторов персональных данных:

- предотвращение утечки информации ограниченного доступа по техническим каналам;

- предотвращение несанкционированного уничтожения, искажения, блокирования, подделки информации;

- обеспечение эффективного управления информационными ресурсами и их использования;

- обеспечение правового режима использования информационных ресурсов, как объекта собственности.

**6. Категории обрабатываемых персональных данных.**

6.1. В информационной системе ПДн Оператора обрабатываются следующие категории ПДн:

6.1.1. ПДн сотрудников. Административно-управленческий персонал, врачи.

Источники поступления: из первичной документации, предоставляемой самими субъектами персональных данных;

6.1.2. ПДн не сотрудников (Пациенты, лица, состоящие в договорных отношениях с Оператором).

Источники поступления: из первичной документации, предоставляемой самими субъектами персональных данных.

6.1.3. Основные сведения об обрабатываемых данных:

|  |  |  |  |
| --- | --- | --- | --- |
| Субъекты ПДн | Цели обработки | Категории ПДн | Правовые основания обработки |
| Сотрудники  учреждения | Реализация трудовых  отношений, начисление заработной платы,  передача информации в налоговые органы,  Пенсионный Фонд | Ф.И.О.; пол; ИНН; СНИЛС; паспортные данные; дата и место рождения; гражданство; сведения об образовании; сведения о работе; адреса; телефоны; сведения о воинском учете; семейное, социальное, имущественное положение; данные  близких родственников; доходы; фотография. | Гражданский кодекс РФ от 30.11.1994 № 51-ФЗ; Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Налоговый Кодекс РФ часть первая от 31 июля 1998г. № 146-ФЗ и часть вторая от 5 августа 2000г. № 117-ФЗ; |
| Кандидаты на  вакантную  должность | Принятие решения о  трудоустройстве, формирование кадрового резерва | Ф.И.О.; паспортные данные; дата и место  рождения; сведения об образовании; сведения о работе; адреса; телефоны; сведения о воинском учете; семейное, социальное, имущественное положение; доходы; данные близких родственников. | Согласие на обработку персональных  данных |
| Граждане | Обеспечение реализации государственной политики в области охраны здоровья населения | Ф.И.О.; пол; ИНН; СНИЛС; паспортные данные; дата и место рождения; гражданство; сведения об образовании; сведения о работе; адреса;  телефоны; сведения о воинском учете; семейное, социальное, имущественное положение; данные  близких родственников | Федеральный закон от 21 ноября 2011г. № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" «О медицинском страховании граждан в Российской Федерации» № 1499-1 |

**7. Принципы обработки персональных данных.**

7.1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в ст. 5 Федерального закона 152-ФЗ «О персональных данных».

7.2. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных.

7.3. Обработка персональных данных Оператором осуществляется на основе следующих принципов:

7.3.1 Обработка персональных данных осуществляется на законной и справедливой основе;

7.3.2 Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

7.3.3 Обработке подлежат только те персональные данные, которые отвечают целям их обработки;

7.3.4 Содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям обработки;

7.3.5 При обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки.

7.3.6 Сроки хранения персональных данных соответствуют нормам, установленным законодательством.

**8. Сведения о третьих лицах, участвующих в обработке персональных данных.**

8.1. В целях соблюдения законодательства РФ, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Оператор в ходе своей деятельности предоставляет персональные данные следующим организациям:

8.1.1. Федеральной налоговой службе.

8.1.2. Пенсионному фонду Российской Федерации.

8.1.3. Территориальному фонду обязательного медицинского страхования Российской Федерации.

8.1.4. Департамент здравоохранения Воронежской области.

8.1.5. БУЗ ВО «Воронежский медицинский информационно-аналитический центр».

8.1.8. Управлению Федерального казначейства по Воронежской области.

**9. Меры по обеспечению безопасности персональных данных**

**при их обработке.**

9.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

9.1.1. Назначением ответственных за организацию обработки персональных данных.

9.1.2. Осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам.

9.1.3. Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и (или) обучением сотрудников.

9.1.4. Определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

9.1.5. Применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных.

9.1.6. Учетом машинных носителей персональных данных.

9.1.7. Выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер.

9.1.8. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

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

9.1.10. Контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

9.1.11. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

9.2. Обязанности должностных лиц, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются в «Положении об обеспечении безопасности персональных данных» и локально утверждённых специальных инструкциях.

**10. Права субъектов персональных данных.**

10.1. В соответствии с №152-ФЗ «О персональных данных» субъект персональных данных имеет право:

10.1.1. Получить сведения касающиеся обработки ПДн оператором:

- 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;

- персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных №152-ФЗ «О персональных данных»;

- информацию об осуществленной или предполагаемой трансграничной передаче данных;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные №152-ФЗ «О персональных данных» или другими федеральным и законами.

10.1.2. Потребовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

10.1.3. Заявить возражение против принятия в отношении себя решений, порождающих юридические последствия на основе исключительно автоматизированной обработки персональных данных.

10.1.4. Отозвать согласие на обработку персональных данных в предусмотренных законом случаях.

10.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами РФ.

10.3. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Тот рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

10.4. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

10.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

**11. Контроль н надзор за обработкой персональных данных.**

11.1. Ответственным за организацию обработки и обеспечения безопасности персональных данных в БУЗ ВО «Воронежский областной клинический центр профилактики и борьбы со СПИД» является лицо, назначенное приказом главного врача учреждения.

11.2. Уполномоченным органом по защите прав субъектов персональных данных, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», является федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

11.3. Уполномоченный орган по защите прав субъектов персональных данных рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение.

**12. Заключительные положения.**

12.1. Настоящая политика утверждается главным врачом учреждения.

12.2. Оператор имеет право вносить изменения в настоящую Политику.

12.3. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее утверждения и размещения на сайте Оператора, если иное не предусмотрено новой редакцией Политики.