Приложение

УТВЕРЖДЕНА

приказом БУЗ ВО «Детский специализированный психоневрологический санаторий»

 от 01.09.2022 №1-2/50-1

**ПОЛИТИКА**

**в отношении обработки персональных данных и реализации требований к защите персональных данных в БУЗ ВО «Детский специализированный психоневрологический санаторий»**

1. **Общие положения**

Настоящая Политика в отношении обработки персональных данных и реализации требований к защите персональных данных (далее - Политика) разработана в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ) и определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных в БУЗ ВО «Детский специализированный психоневрологический санаторий» (далее - Учреждение) с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную, семейную и врачебную тайну.

В настоящей Политике используются следующие термины и определения:

1) персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) 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;

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;

4) автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

5) распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

6) предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

7) блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

8) 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;

9) обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

10) информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

11) общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Действие Политики распространяется на все персональные данные субъектов, обрабатываемые в Учреждении с использованием средств автоматизации, а также без использования таких средств.

Настоящая Политика является общедоступной и подлежит публикации на официальном сайте Учреждения или иметь неограниченный доступ всех субъектов персональных данных.

1. **Цели обработки персональных данных**

Обработка персональных данных в Учреждении осуществляется в целях:

- осуществления кадровой работы в Учреждении в соответствии с требованиями трудового законодательства Российской Федерации;

- оказание медицинских услуг пациентам в соответствии с Федеральным законом от 21 ноября 2011 г. № 323 – ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

1. **Принципы обработки персональных данных**

Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

1) законной и справедливой основе;

2) ограничение обработки персональных данных достижением конкретных, заранее определенных и законных целей;

3) недопущение объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

4) обработка только тех персональных данных, которые отвечают целям их обработки;

5) соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;

6) недопущение обработки избыточных персональных данных по отношению к заявленным целям их обработки;

7) обеспечение точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;

Учреждение осуществляет обработку персональных данных только с письменного согласия работников и пациентов - субъектов персональных данных на обработку их персональных данных.

Безопасность персональных данных достигается путем исключения 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.

1. **Обрабатываемые персональные данные**

Учреждение осуществляет обработку персональных данных работников Учреждения с письменного согласия в случаях установленных ст.11 Закона № 152-ФЗ.

Обработка специальных категорий персональных данных, касающихся состояния здоровья, ведется на пациентов при оказании медицинской услуги.

Обработка ведется с письменного согласия пациента в соответствии ст.ст. 6,9,10 Закона №152 – ФЗ, ч.3 ст.13 Закона № 323 – ФЗ.

В целях информационного обеспечения в Учреждении создаются общедоступные источники персональных данных, в том числе справочники, адресные и телефонные книги. В общедоступные источники персональных данных с согласия работника могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адреса электронной почты и иные персональные данные, сообщаемые субъектом персональных данных.

1. **Условия обработки персональных данных**

Работники Учреждения, допущенные к обработке персональных данных на основании правовых актов Учреждения, осуществляют обработку персональных данных после ознакомления с нормативными актами Учреждения, регламентирующими порядок и процедуры работы с персональными данными.

Доступ работников Учреждения, допущенных к обработке персональных данных, к категориям персональных данных, обрабатываемых в ИСПДн, осуществляется на основании Положения о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных Учреждения, которым определяется список лиц, ответственных за обработку персональных данных в ИСПДн Учреждения, а также их уровень прав доступа к обрабатываемым персональным данным.

Оператор не предоставляет и не раскрывает сведения, содержащие персональные данные субъектов, третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральными законами.

Персональные данные хранятся в электронном виде в составе информационных систем персональных данных (далее - ИСПДн), в составе архивных копий баз данных ИСПДн и на бумажных носителях.

При обработке и хранении персональных данных соблюдаются организационные и технические меры, обеспечивающие их сохранность и исключающие несанкционированный доступ к ним, к которым относятся:

1. назначение работника Учреждения, ответственного за организацию обработки персональных данных, и за обеспечение безопасности персональных данных при их обработке в ИСПДн;
2. ограничение физического доступа к местам хранения персональных данных в бумажном виде и носителям информации в электронном виде;
3. соблюдение правил обработки персональных данных в ИСПДн;
4. применение сертифицированных средств защиты информации.
5. **Обеспечение безопасности персональных данных**

Обеспечение безопасности персональных данных в Учреждении достигается следующими мерами:

1. назначение работника Учреждения, ответственного за организацию обработки персональных данных, и за обеспечение безопасности персональных данных при их обработке в ИСПДн;

2) определение угроз безопасности персональных данных, разработка на их основе частной модели угроз безопасности персональных данных и разработка системы защиты персональных данных для соответствующего класса ИСПДн;

3) назначение администраторов безопасности ИСПДн;

4) реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;

5) применение сертифицированных средств защиты информации;

6) осуществление антивирусного контроля;

7) парольная защита доступа к ИСПДн;

8) резервное копирование;

9) обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

10) ведение электронного журнала регистрации действий пользователей ИСПДн;

11) разработка и утверждение локальных актов Учреждения, регламентирующих порядок обработки персональных данных, разработка инструкций;

12) обучение работников Учреждения, допущенных к обработке персональных данных, и использующих средства защиты информации, правилам работы с ними;

13) проведение периодических проверок состояния защищенности ИСПДн.

1. **Права субъекта персональных данных**

 Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, за исключением случаев, когда право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральным законодательством.

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

1) подтверждение факта обработки персональных данных 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) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Получение данной информации осуществляется на основании письменного запроса субъекта персональных данных в Учреждение.

Ответ, содержащий запрашиваемую информацию, либо мотивированный отказ в ее предоставлении направляется субъекту по адресу, указанному в запросе, в течение 30 дней.

Порядок обработки запросов субъектов персональных данных по выполнению их законных прав осуществляется в соответствии с локальными актами Учреждения.

1. **Обязанности**

Учреждение обязуется осуществлять обработку персональных данных только с согласия субъектов персональных данных, за исключением случаев, предусмотренных Законом № 152-ФЗ.

При сборе персональных данных Учреждение обязуется по запросу субъекта персональных данных предоставлять последнему информацию, касающуюся обработки его персональных данных, в соответствии с положениями настоящей Политики. В случае, если предоставление персональных данных субъектом персональных данных является обязательным в соответствии с федеральным законодательством, Учреждение обязуется разъяснять субъекту персональных данных юридические последствия отказа от предоставления персональных данных.

Учреждение при обработке персональных данных обязуется принимать необходимые правовые, организационные и технические меры 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.

Учреждение обязуется отвечать на запросы субъектов персональных данных, их законных представителей, а также уполномоченного органа по защите прав субъектов персональных данных в части обрабатываемых персональных данных в соответствии с требованиями законодательства.

В случае предоставления субъектом персональных данных, либо его представителем сведений, подтверждающих факты каких-либо нарушений в процессе обработки персональных данных, Учреждение обязуется устранить данные нарушения в течение семи рабочих дней и уведомить субъекта персональных данных о внесенных изменениях и принятых мерах.

Учреждение обязуется уведомлять уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных Законом № 152-ФЗ.