

**УТВЕРЖДАЮ**

И.О. Главного врача Государственного  
бюджетного учреждения здравоохранения  
города Москвы «Детский бронхолегочный  
санаторий №27 ДЗМ»



Дубовицкая Е.С.

09 января 2023 года

М.П.

**Политика обработки и защиты персональных данных  
медицинской организации  
ГБУЗ «Детский бронхолегочный санаторий №27 ДЗМ»**

**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 № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом медицинской организации ГБУЗ «Детский бронхолегочный санаторий №27 ДЗМ» (далее Учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее ПДн) оператором которых является Учреждение в целях исполнения требований Федерального Закона от 27.06.2006.№ 152-ФЗ «О персональных данных».
- 1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты персональных данных, необходимых для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, направлена на обеспечение защиты прав и свобод человека и гражданина при обработке ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и соблюдение врачебной тайны.
- 1.3. Положение Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.
- 1.4. Обработка ПДн в Учреждении осуществляется в связи с выполнением Учреждением функций, предусмотренных ее учредительными документами, и определяемых:
  - Федеральным законом от 21 ноября 2011г. №323-ФЗ «Об основах охраны здоровья граждан в РФ».
  - Федеральным законом №152-ФЗ от 27 июля 2006г «О персональных данных» (далее Федеральный закон о персональных данных);
  - Постановлением Правительства РФ от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

- Постановлением Правительства РФ от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

- иным нормативным правовым актом РФ.

Кроме того, обработка ПДн в учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя (глава 14 Трудового кодекса РФ), в связи с реализацией Учреждением своих прав и обязанностей как юридического лица.

- 1.5. Учреждение 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, если иное не предусмотрено новой редакцией Политики.
- 1.6. Действующая редакция хранится в месте нахождения Учреждения по адресу: Московская область, Раменский городской округ, рабочий поселок Ильинский, улица Октябрьская д 14., электронная версия Политики – на сайте по адресу: detsan27.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 и 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.

**Оператор** — государственных 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.

**Распространение персональных данных-** действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**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 невозможно восстановить содержание персональных данных в информационной

системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

**Информационная система персональных данных (ИСПДн)** — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Пациент** — физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

**Медицинская деятельность** — профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

**Лечащий врач** - врач, на которого возложена функция по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

### **3. Принципы обеспечения безопасности персональных данных**

3.1 Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении является **предотвращение несанкционированного доступа к ним третьих лиц**, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2 Для обеспечения безопасности ПДн Учреждение руководствуется следующими принципами:

— **Законность**: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов области обработки и защиты ПДн;

— **системность**: обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

— **комплексность**: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных

системах Учреждения и других имеющихся в Учреждении систем и средств защиты;

- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работника в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн представляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Учреждения, а также обмена и состава обрабатываемых ПДн;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляется Работниками, имеющим необходимые квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- наблюдаемость и прозрачность: меры по обеспечению ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющие контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

3.3 В Учреждении не производится обработка ПДн, несовместимая с целями их сбора. Если иное предусмотрено федеральным законом, по окончании обработки ПДн в Учреждении, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Учреждением ПДн уничтожаются или обезличиваются.

3.4 При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

## **4. Обработка персональных данных**

### **4.1 Получение ПДн**

4.1.1 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.

4.1.2 Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3 Документы, содержащие ПДн, создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др);

б) внесение сведений в учетные формы;

в) получения оригиналов необходимых документов ( трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Учреждением, определяется в соответствии с законодательством и внутренними регулятивным и документами Учреждения.

## **4.2. Обработка ПДн**

4.2.1 Обработка персональных данных осуществляется:

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

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

Учреждением производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

#### **4.2.2. Цели обработки ПДн:**

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральным законом от 21 ноября 2011 № 323 - ФЗ « Об основах охраны здоровья граждан РФ» , от 21 апреля 2010 № 61-ФЗ « об обращении лекарственных средств» и от 29 ноября 2010 № 326-ФЗ « об обязательном медицинском страховании граждан в РФ»
- осуществление трудовых отношений.

#### **4.2.3. Категории субъектов персональных данных**

В Учреждении обрабатываются ПДн следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, обратившиеся в учреждение за медицинской помощью.

#### **4.2.4 ПДн, обрабатываемые Учреждением:**

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу в Учреждение;
- данные, полученные при оказании медицинской помощи.

#### **4.2.5. Обработка персональных данных ведется:**

Обработка персональных данных ведется:

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

Обработка персональных данных должна осуществляться на основе принципов:

- Законности целей и способов обработки персональных данных и добросовестности;
  - соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
  - соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
  - достоверности персональных данных, их достаточности для целей обработки.
- Недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных.

### **4.3. Хранение ПДн**

- 4.3.1 ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.
- 4.3.2 ПДн, зафиксированные на бумажных носителях, хранятся запираемых шкафах.
- 4.3.3 ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках.
- 4.3.4 Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменниках) в ИСПД.
- 4.3.5 Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели из обработки, и они подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в их достижении.

### **4.4. Уничтожение ПДн**

- 4.4.1 Уничтожение документов (носителей), содержащих ПДн, производится путем дробления (измельчения).
- 4.4.2 ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.
- 4.4.3 Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

### **4.5. Передача ПДн**

4.5.1 Учреждение передает ПДн третьим лицам в следующих случаях:

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

4.5.2. Перечень лиц, которым передаются ПДн:

- Пенсионный фонд РФ для учета (на законных основаниях).
- Налоговый орган РФ (на законных основаниях).
- Фонд социального страхования (на законных основаниях).
- Территориальный фонд обязательного медицинского страхования (на законных основаниях).
- Страховые медицинские организации по обязательному медицинскому страхованию (на законных основаниях).
- Банки для начисления заработной платы (на основании договора).
- Судебные и правоохранительные органы в случаях, установленных законодательством.
- Военные комиссариаты (на законных основаниях).

## 5. Защита персональных данных

- 5.1 В соответствии с требованиями нормативных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты
- 5.2 Подсистема правовой защиты представляет собой комплекс правовых, организационно- распорядительных и нормативных документов, обеспечивающих — создание, функционирование и совершенствование СЗПД.
- 5.3 Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.
- 5.4 Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн
- 5.5 Основными мерами защиты ПДн, используемыми Учреждением, являются:
  - 5.5.1 Назначение лиц, ответственного за обработку ПДн, которые осуществляют организацию обработки ПДн, внутренний контроль за соблюдением Учреждением и его работниками требований к защите ПДн.
  - 5.5.2 Определение актуальных угроз безопасности ПДн при их обработке и ИСПД и разработка мер и мероприятий по защите ПДн.
  - 5.5.3 Разработка политики в отношении обработки персональных данных
  - 5.5.4 Установление прав доступа к ПДн, обрабатываемым в ИСПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПД.
  - 5.5.5 Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.
  - 5.5.6 Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
  - 5.5.7 Сертифицированное программное средство защиты информации от несанкционированного доступа.
  - 5.5.8 Соблюдение условий, обеспечивающих сохранность ПДн и исключаящие несанкционированный доступ.
  - 5.5.9 Установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к ПДн и принятия мер.
  - 5.5.10 Восстановление ПДн, модифицированных или уничтоженных — вследствие несанкционированного доступа к ним.
  - 5.5.11 Обучение работников Учреждения непосредственно осуществляющих обработку персональных данных положениям Законодательства РФ о персональных данных, в том числе, требованиям к защите ПДн, документам определяющим политику Учреждения в отношении обработки ПД, локальным актам по вопросам обработки ПДн.
  - 5.5.12 Осуществление внутреннего контроля и аудита.



## 6. Основные права субъекта ПДн и обязанности Учреждения

### 6.1. Основные права субъекта ПДн:

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

- подтверждение факты обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты ПДн на основании договора с оператором или на основании Федерального Закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных ФЗ «О персональных данных»;
- иные сведения, предусмотренные настоящим Федеральным законом или другими Федеральными законами.

Субъект ПДн вправе требовать от оператора уточнения его ПДн, их блокирование или уничтожение в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

### 6.2. Обязанности Учреждения

Учреждение обязано:

- при сборе ПДн предоставить информацию об обработке его ПДн;
- в случае если ПДн были получены не от субъекта ПДн уведомить субъекта;
- при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа;
- опубликовывать 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, представления, распространения ПДн, 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.