



Утверждаю

Главный врач ГБУ РО «ГП № 16»

в г. Ростове-на-Дону

Д.В. Стагниев

30 сентября 2022 года

Политика обработки и защиты персональных данных медицинской организации ГБУ РО «ГП № 16» в г. Ростове-на-Дону

1. Общие положения

1.1 Настоящая Политика в отношении 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 ГБУ РО «ГП № 16» в г. Ростове-на-Дону (далее- Организация или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее -ПД), оператором которых является Организация.

1.2 . Политика разработана в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Организацией как до, так и после утверждения настоящей Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПД, полученных до её утверждения.

1.4. Обработка ПД в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами, и определяемых:

- Конституцией РФ;
- Трудовым кодексом РФ;
- Федеральным законом от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом №152-ФЗ от 27 июля 2006 года «О персональных данных»;
- Федеральным законом № 149-ФЗ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

-Постановлением Правительства Российской Федерации 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»;

-иными нормативными правовыми актами Российской Федерации.

Обработка ПД в Организации осуществляется в связи с оказанием Организацией медицинских услуг.

Кроме того, обработка ПД в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Действующая редакция хранится в месте нахождения Организации по адресу: Ростовская область, г. Ростов-на-Дону, пр-кт Космонавтов 6/1, электронная версия Политики – *на сайте по адресу: <https://poll6.ru/>*

2. Термины и принятые сокращения

Персональные данные (ПД)- любая информация, относящаяся прямо или косвенно к 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, копирование, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение 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.

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

Предоставление персональных данных- действия, направленные на раскрытие персональных данных 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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных – действие, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных к конкретному субъекту персональных данных.

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

Информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических 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, проведение медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санаторно—противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) её компонентов в медицинских целях.

Лечащий врач – врач, на которого возложены функции 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 ПД при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно - технических и

иных воздействий с целью хищения ПД, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПД Организация руководствуется следующими принципами:

- Законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;
- Системность: обработка ПД в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания решения проблемы обеспечения безопасности ПД;
- Комплексность защиты ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- Непрерывность: защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе проведения ремонтных и регламентных работ;
- Своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;
- Преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляются на основании результатов анализа практики обработки ПД в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;
- Персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД;
- Минимизация прав доступа : доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей.
- Гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПД;
- Специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляется Работниками, имеющими необходимые квалификацию и опыт;
- Эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивации и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;
- Наблюдаемость и прозрачность : меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты применения были

явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль; непрерывность контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.

3.3. В Организации не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено Федеральным законом, по окончании обработки ПД в Организации, в том числе при достижении целей их обработки или утраты необходимости и достижения этих целей, обрабатывавшиеся в Организации ПД уничтожаются или обезличиваются.

3.4. При обработке ПД обеспечиваются их точность, достаточность, а при необходимости и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уничтожению неполных или неточных ПД.

4. Обработка персональных данных

4.1. Получение ПД

4.1.1. Все ПД следует получать от самого субъекта. Если ПД 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 ПД, характере подлежащих получению ПД, перечне действий с ПД, сроке, в течение которого действует согласие, и порядок его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПД, 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.).

Порядок доступа субъекта ПД к его ПД, обрабатываемым Организацией, определяется в соответствии с законодательством РФ.

4.2. Обработка ПД

4.2.1. 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).

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

Допущенные к обработке ПД Работники под подпись знакомятся с документами Организации, устанавливающими порядок обработки ПД.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПД.

4.2.2. Цели обработки ПД:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательства и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. №323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. №61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года №326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными постановлением Правительства Российской Федерации от 11.05.2023 г. № 736;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПД следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью, включая законных представителей пациентов.

4.2.4. ПД, обрабатываемые Организацией;

- данные, полученные при осуществлении трудовых отношений;
- данные, полученные для осуществления отбора кандидатов на работу в Организацию;

- данные, полученные при осуществлении гражданско-правовых отношений;
- данные, полученные при оказании медицинской помощи.

- 4.2.5. Обработка персональных данных ведется;
- с использованием средств автоматизации;
 - без использования средств автоматизации.

4.3. Хранение ПД

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

4.3.2. ПД, зафиксированные на бумажных носителях, хранятся в помещениях с ограниченным правом доступа.

4.3.3. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.4. Хранение ПД в форме, позволяющей определить субъекта ПД, 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.

4.4. Уничтожение ПД

4.4.1. Уничтожение документов (носителей), содержащих ПД, производится посредством сдачи предприятию на утилизацию вторсырья.

4.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении ПД, подписанным членами комиссии.

4.5. Передача ПД

4.5.1. Организация передает ПД третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;
- передача предусмотрена законодательством РФ.

4.5.2. Перечень лиц, которым передаются ПД:

- социальный фонд России (на законных основаниях);
- бюро медико-социальной экспертизы;
- страховые медицинские организации (на законных основаниях);
- другие организации в рамках законодательства РФ.

5. Защита ПД

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной, технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых организационных, 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, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитические работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно - аппаратных средств, обеспечивающих защиту ПД.

5.5. Основными мерами защиты ПД, используемыми Организацией, являются:

5.5.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД.

5.5.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД, и разработка мер и мероприятий по защите ПД.

5.5.3. Разработка политики в отношении обработки персональных данных.

5.5.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПД в ИСПД.

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

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПД, обеспечение их сохранности.

5.5.7. Сертифицированное программное средство защиты информации от несанкционированного доступа

5.5.8. Сертифицированный межсетевой экран и средство обнаружения вторжения.

5.5.9. Соблюдение условий, обеспечивающих сохранность ПД и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПД.

5.5.10. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

6. Основные права субъекта ПД и обязанности Организации

6.1. Основные права субъекта ПД

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

- 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;
- обрабатываемые 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, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о 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 настоящим Федеральным законом или другими федеральными законами.

Субъект ПД вправе требовать 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, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности Организации

Организация обязана:

- при сборе ПД предоставлять информацию об обработке его ПД;
- в случаях если ПД были получены не от субъекта ПД уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.