Приложение № 5
к приказу № 2-ОТД от «19» 08 2024г.

Утверждаю
Директор ООО «Медикал Парк»
_____ А.Ш.Шамилева

Политика обработки и защиты персональных данных
в ООО « Медикал Парк»

1. Общие положения

1.1. Настоящая Политика обработки и защиты персональных данных (далее – Политика) определяет порядок обработки персональных данных (далее – ПД) и меры по обеспечению безопасности персональных данных в ООО «Медикал Парк» с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, гарантируемых Конституцией.
1.2. Настоящая Политика является локальным нормативным актом ООО «Медикал Парк» (далее – Клиника) и разработана в соответствии с Федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных» и Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; постановлениями Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; приказом ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», главой 14 ТК РФ.
1.3. Настоящая Политика раскрывает принципы, порядок и условия обработки ПД физических лиц при обращении за медицинской помощью в Клинику. Кроме того, обработка ПД осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Клиника выступает в качестве работодателя (гл. 14 ТК), в связи с реализацией своих прав и обязанностей как юридического лица.
1.4. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Клиникой 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 ПД, полученных до ее утверждения.
1.5. Клиника 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 Политики хранится в месте нахождения Клиники по адресу: 295050, Республика крым, г. Симферополь, ул. Кечкеметская, д.53, электронная версия Политики – на сайте по адресу: медикал-парк.рф.
1.7. Персональные данные обрабатывают с использованием средств автоматизации или без них.
1.8. Клиника до начала обработки персональных данных обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных согласно частям 1 и 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
1.9. Ответственный за организацию обработки персональных данных в Клинике назначается Приказом директора, в соответствии с пунктом 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ (далее - ФЗ №152).

2. Термины и принятые сокращения

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

2.2. Персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном ФЗ №152.

2.3. 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

2.4. 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.

2.5. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.6. Распространение персональных данных – действия, направленные на раскрытие персональных данных не определенному кругу лиц.

2.7. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.8. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.9. 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.

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

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

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

2.13. 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.

2.14. Лечащий врач – врач, на которого возложены функции по Клиникеи непосредственному оказанию Потребителю/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 Клинике 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 Клиника руководствуется следующими принципами:
3.2.1. Законность – защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД.
3.2.2. Системность – обработка ПД в Клинике осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД.
3.2.3. Комплексность – защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Клинике и других имеющихся в Клинике систем и средств защиты.
3.2.4. Непрерывность – защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных и регламентных работ.
3.2.5. Своевременность – меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки.
3.2.6. Преемственность и непрерывность совершенствования – модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в Клинике с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации.
3.2.7. Персональная ответственность – ответственность за обеспечение безопасности ПД возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД.
3.2.8. Минимизация прав доступа – доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей.
3.2.9. Гибкость – обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Клиники, а также объема и состава обрабатываемых ПД.
3.2.10. Специализация и профессионализм – реализация мер по обеспечению безопасности ПД осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт.
3.2.11. Эффективность процедур отбора кадров – кадровая политика Клиники предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД.
3.2.12. Наблюдаемость и прозрачность – меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль.
3.2.13. Непрерывность контроля и оценки – устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.
3.3. Безопасность ПД, обрабатываемых Организацией, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты ПД.
3.4. Меры по обеспечению безопасности ПД включают в себя, в частности:
- назначение ответственного за организацию обработки ПД;
- издание локальных правовых актов, регулирующих права и обязанности оператора ПД, описывающих систему мер по защите ПД, определяющих доступ к информационным системам ПД;
- определение угроз безопасности ПД при их обработке в информационных системах ПД;
- применение методов (способов) защиты информации;

- ознакомление сотрудников с законодательными актами и внутренними документами, регламентирующими порядок работы с ПД;
- обучение сотрудников правилам обработки данных и процедурам безопасной работы;
- организацию работы с субъектами персональных данных и контрагентами: заключение соглашений о конфиденциальной информации, выдача поручения обрабатывать ПД, получение согласия субъектов;
- учет машинных носителей ПД;
- обнаружение фактов несанкционированного доступа к ПД и принятие мер;
- своевременное выявление и устранение нарушений требований к порядку работы с ПД;
- регулярное изменение паролей на компьютерах и в информационных системах, которые используются для обработки ПД;
- восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- организация рабочих помещений, в которых хранится и обрабатывается носитель ПД: введение пропускного режима, оборудование сейфов и специально отведённых мест;
- установление правил доступа к ПД, обрабатываемым в информационной системе ПД, а также обеспечение регистрации и учета всех действий, совершаемых с ПД в информационной системе ПД;
- контроль принимаемых мер по обеспечению безопасности ПД и уровня защищенности информационных систем ПД;
- анализирование защищённости на рабочих терминалах и серверах, принятие мер по устранению выявленных недостатков, усиление защитных мер;
- управление доступом к персональным данным: протоколирование действий с ПД, оповещение о несанкционированном доступе в систему
- и иные организационные и технические меры.

3.5. В Клинике не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД в Клинике, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Клиникой ПН уничтожаются или обезличиваются.

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

4. Порядок обработки персональных данных в Организации

4.1. Категории ПД

В Клинике обрабатываются следующие ПД:

- фамилия, имя, отчество (при наличии), а также прежние фамилия, имя, отчество (при наличии), дата и место их изменения (в случае изменения);
- пол;
- дата (число, месяц, год) и место рождения;
- данные изображения лица, полученные с помощью фото- видео устройств, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;
- фотографическое изображение;
- сведения о гражданстве;
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- страховой номер индивидуального лицевого счета (СНИЛС);
- идентификационный номер налогоплательщика (ИНН);
- данные документа, содержащиеся в свидетельстве о рождении;
- адрес и дата регистрации по месту жительства (месту пребывания), адрес фактического проживания;

- номер контактного телефона, адрес электронной почты и (или) сведения о других способах связи;
- серия и номер страхового полиса ДМС;
- реквизиты свидетельств о государственной регистрации актов гражданского состояния и содержащиеся в них сведения;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты (число, месяц, год) и места рождения);
- сведения об образовании и (или) квалификации или наличии специальных знаний (в том числе наименование образовательной и (или) иной организации, год окончания, уровень образования, квалификация, реквизиты документа об образовании, обучении);
- информация о владении иностранными языками;
- сведения об отношении к воинской обязанности, о воинском учете и реквизиты документов воинского учета (серия, номер, дата выдачи документа, наименование органа, выдавшего его);
- сведения о трудовой деятельности, а также информация о предыдущих местах работы, периодах и стаже работы, профессии, должности; данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации);
- данные водительского удостоверения;
- сведения, содержащиеся в документах, дающих право на пребывание и трудовую деятельность на территории РФ (для иностранных граждан, пребывающих в РФ);
- сведения, содержащиеся в разрешении на временное проживание, разрешении на временное проживание в целях получения образования (для иностранных граждан, временно проживающих в РФ), виде на жительство (для иностранных граждан, постоянно проживающих в РФ);
- сведения о доходах, обязательствах по исполнительным документам;
- номера расчетного счета, лицевого счета, реквизиты банковской карты;
- сведения о состоянии здоровья (для отдельных категорий работников);
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (для отдельных категорий работников);
- пенсионное удостоверение;
- иные персональные данные, содержащиеся в документах, представление которых предусмотрено законодательством, если обработка этих данных соответствует цели обработки, предусмотренной п. 3.1 настоящей Политики;
- иные персональные данные, которые работник пожелал сообщить о себе и обработка которых соответствует цели обработки, предусмотренной п. 3.1 настоящей Политики.

4.2. Цели обработки ПД:

4.2.1. Обеспечение Клиникой оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими Клиниками платных медицинских услуг, утвержденными постановлением Правительства Российской Федерации от 11.05.2023 № 736 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг, внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившим силу постановления Правительства Российской Федерации от 4 октября 2012 г. №1006».

4.2.2. Осуществление трудовых отношений.

4.2.3. Осуществление гражданско-правовых отношений.

4.2.4. Выполнение договорных обязательств.

4.3. Категории субъектов ПД

4.3.1. В Клинике обрабатываются ПД следующих субъектов:

- физические лица, состоящие с Клиникой в трудовых отношениях;
- физические лица, уволившиеся из Клиники;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с Клиникой в гражданско-правовых отношениях;
- физические лица, обратившиеся в Клинику за медицинской помощью, их законные представители;
- контрагенты;
- выгодоприобретатели по заключенным с Клиникой договорам;
- иные категории субъектов персональных данных, персональные данные которых обрабатываются;

4.4. ПД, обрабатываемые Клиникой

4.4.1. В Клинике обрабатываются ПД:

- полученные при осуществлении трудовых отношений;
- полученные для осуществления отбора кандидатов на работу в Организацию;
- полученные при осуществлении гражданско-правовых отношений;
- полученные при оказании медицинской помощи.

4.3. Получение ПД

4.3.1. 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.

4.3.2. 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 порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.3.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) ПД в Клинике осуществляются посредством:

- получения оригиналов документов либо их копий (трудовая книжка, медицинское заключение, характеристика и т. д.);
- внесения сведений в учетные формы на бумажных и электронных носителях;
- создания документов, содержащих персональные данные, на бумажных и электронных носителях;
- внесения ПД в информационные системы ПД.

4.4. Обработка ПД

4.4.1. Обработка персональных данных осуществляется путем Сбора, Записи, Систематизации, Накопления, Хранения, Уточнения (обновления, изменения), Извлечения, Использования, Передача (предоставление, доступ), Обезличивания, Блокирования, Удаления, Уничтожения персональных данных, в том числе с помощью средств вычислительной техники.

4.4.2. До начала обработки ПД Клиника обязана уведомить Роскомнадзор о намерении осуществлять обработку ПД.

4.4.3. Обработка персональных данных в Клинике выполняется следующими способами:

- неавтоматизированная обработка ПД;
- автоматизированная обработка ПД с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка ПД.

4.4.4. Обработка персональных данных осуществляется:

4.4.4.1. С согласия субъекта ПД на обработку его ПД, если иное не предусмотрено законодательством в области ПД.

4.4.4.2. В случаях, когда обработка ПД необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей.

4.4.4.3. В случаях, когда осуществляется обработка ПД, доступ неограниченного круга лиц к которым предоставлен субъектом ПД либо по его просьбе (далее – ПД, сделанные общедоступными субъектом ПД).

4.4.4.4. Обработка ПД, разрешенных субъектом ПД для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 ФЗ №152. Согласие на обработку таких ПД оформляется отдельно от других согласий на обработку ПД. Согласие предоставляется субъектом ПД лично либо в форме электронного документа, подписанного электронной подписью, с использованием информационной системы Роскомнадзора.
4.4.4.5. Обработка биометрических ПД допускается только при наличии письменного согласия субъекта ПД. Исключение составляют ситуации, предусмотренные ч. 2 ст. 11 ФЗ №152.
4.4.5. В Клинике для обработки ПД используются следующие информационные системы:

- корпоративная электронная почта;
- электронные медицинские карты;
- система электронного документооборота;
- система поддержки рабочего места пользователя;
- системы управления медицинскими записями;
- система нормативно-справочной информации;
- система управления персоналом;
- система контроля за удаленным доступом;
- информационный портал.

4.4.6. Передача (распространение, предоставление, доступ) ПД субъектов ПД осуществляется в случаях и в порядке, предусмотренных законодательством в области ПД и настоящей Политикой.
4.4.7. Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПД.

4.5. Хранение ПД

4.5.1. ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.
4.5.2. 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. Исключение – случаи, когда срок хранения ПД установлен федеральным законом, договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект ПД.
4.5.3. ПД на бумажных носителях хранятся в Клинике в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», перечень типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения, утв. приказом Росархива от 20.12.2019 № 236).
4.5.4. Срок хранения ПД, обрабатываемых в информационных системах ПД, соответствует сроку хранения ПД на бумажных носителях.
4.5.5. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).
4.5.6. ПД субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).
4.5.7. Не допускается хранение и размещение документов, содержащих ПД, открытых электронных каталогах (файлообменниках) в ИСПД.

4.6. Прекращение обработки ПД

4.6.1. Обработка ПД в Клинике прекращается в следующих случаях:

- при выявлении факта неправомерной обработки ПД. Срок прекращения обработки – в течение трех рабочих дней со дня выявления такого факта.Если обеспечить правомерность обработки невозможно, оператор в течение 10 рабочих дней должен уничтожить персональные данные и уведомить об этом субъекта персональных данных или его представителя
- при достижении целей обработки ПД (за некоторыми исключениями);

- по истечении срока действия или при отзыве субъектом ПД согласия на обработку его ПД (за некоторыми исключениями), если в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ их обработка допускается только с согласия;
- при обращении субъекта ПД к Клиникес требованием о прекращении обработки ПД (за исключением случаев, предусмотренных ч. 5.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ). Срок прекращения обработки – не более 10 рабочих дней с даты получения требования (с возможностью продления не более чем на пять рабочих дней, если направлено уведомление о причинах продления).

4.7. Блокирование и уничтожение ПД

4.7.1. Клиника блокирует ПД в порядке и на условиях, предусмотренных законодательством в области ПД.
4.7.2. При достижении целей обработки ПД или в случае утраты необходимости в достижении этих целей ПД уничтожаются либо обезличиваются. Исключение может предусматривать федеральный закон.
4.7.3. Незаконно полученные ПД или те, которые не являются необходимыми для цели обработки, уничтожаются в течение семи рабочих дней со дня представления субъектом ПД (его представителем) подтверждающих сведений.
4.7.4. ПД, обработка которых прекращена из-за ее неправомерности и правомерность обработки которых невозможно обеспечить, уничтожаются в течение 10 рабочих дней с даты выявления факта неправомерной обработки.
4.7.5. ПД уничтожаются в течение 30 дней с даты достижения цели обработки, если иное не предусмотрено договором, стороной которого (выгодоприобретателем или поручителем по которому) является субъект ПД, иным соглашением между ним и Клиникой, либо если Клиника не вправе обрабатывать ПД без согласия субъекта ПД на основаниях, предусмотренных федеральными законами.
4.7.6. При достижении максимальных сроков хранения документов, содержащих ПД, ПД уничтожаются в течение 30 дней.
4.7.7. ПД уничтожаются (если их сохранение не требуется для целей обработки ПД) в течение 30 дней с даты поступления отзыва субъектом ПД согласия на их обработку. Иное может предусматривать договор, стороной которого (выгодоприобретателем или поручителем по которому) является субъект ПД, иное соглашение между ним и Клиникой. Кроме того, ПД уничтожаются в указанный срок, если Клиника не вправе обрабатывать их без согласия субъекта ПД на основаниях, предусмотренных федеральными законами.
4.7.8. Отбор материальных носителей (документы, жесткие диски, флеш-накопители и т.п.) и (или) сведений в информационных системах, содержащих ПД, которые подлежат уничтожению, осуществляет ответственное лицо по работе с персональными данными, обрабатывающие ПД.
4.7.9. Уничтожение персональных данных осуществляет комиссия, созданная приказом директором Клиники.
4.7.9.1. Комиссия составляет список с указанием документов, иных материальных носителей и (или) сведений в информационных системах, содержащих ПД, которые подлежат уничтожению.
4.7.9.2. Уничтожение документов (носителей), содержащих ПД, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.
ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.
ПД на физических электронных носителях уничтожаются путем механического нарушения целостности носителя, не позволяющего считать или восстановить персональные данные, а также путем удаления данных с электронных носителей методами и средствами гарантированного удаления остаточной информации.
Обнуление или перезапись информации до состояния, исключающего восстановление.
Выбор способа зависит от типа носителя и степени чувствительности данных. Закон акцентирует внимание на необходимости исключить возможность восстановления данных любыми способами.

4.7.9.3. Комиссия подтверждает уничтожение ПД, указанных в пунктах 4.7.4 – 4.7.7. настоящей Политики согласно Требованиям к подтверждению уничтожения ПД, утвержденным приказом Роскомнадзора от 28.10.2022 № 179, а именно:

- актом об уничтожении ПД – если данные обрабатываются без использования средств автоматизации;
- актом об уничтожении ПД и выгрузкой из журнала регистрации событий в информационной системе ПД – если данные обрабатываются с использованием средств автоматизации либо одновременно с использованием и без использования таких средств.

Акт может составляться на бумажном носителе или в электронной форме, подписанной электронными подписями.

Формы акта и выгрузки из журнала с учетом сведений, которые должны содержаться в указанных документах, утверждаются приказом директора Клиники.

4.7.9.4. После составления акта об уничтожении ПД и выгрузки из журнала регистрации событий в информационной системе ПД комиссия передает их в общий отдел для последующего хранения.

4.7.9.5. Акты и выгрузки из журнала хранятся в течение трех лет с момента уничтожения персональных данных.

4.8. Передача ПД

4.8.1. Клиника передает ПД третьим лицам, если субъект ПД выразил свое согласие на такие действия или передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

4.8.2. Перечень третьих лиц, которым передаются ПД:

- Социальный фонд РФ для учета (на законных основаниях);
- Налоговые органы РФ (на законных основаниях);
- страховые медицинские Организации по добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций

4.8.3. Клиника не осуществляет трансграничную передачу ПД.

4.9. Доступ к ПД

4.9.1. Порядок доступа субъекта ПД к его ПД, обрабатываемым Клиникой, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Клиники.

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

4.9.3. Допущенные к обработке ПД Работники под подпись знакомятся с документами Клиники, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

5. Защита персональных данных

5.1. Подсистема защиты ПД

5.1.1. В соответствии с требованиями нормативных документов Клиники создана система защиты ПД (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.1.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.1.3. 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, аналитической работы.

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

5.2. Основные меры защиты ПД

Основными мерами защиты ПД, используемыми Клиникой, являются:

5.2.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением Клиникой и ее работниками требований к защите ПД.

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

5.2.3. Разработка политики в отношении обработки ПД.

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

5.2.5. Установление индивидуальных паролей доступа работников в информационную систему в соответствии с их производственными обязанностями.

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

5.2.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.2.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.

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

5.2.10. Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учета действий, совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

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

5.2.12. Обучение работников Клиники, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о ПД, в том числе требованиям к защите ПД, документам, определяющим политику Клиникев отношении обработки ПД, локальным актам по вопросам обработки ПД.

5.2.13. Осуществление внутреннего контроля и аудита.

5.2.14. Работники Клиники, непосредственно осуществляющие обработку ПД, должны быть ознакомлены под подпись до начала работы с положениями законодательства Российской Федерации о ПД, в том числе с требованиями к защите ПД, настоящей Политикой и изменениями к ней, локальными актами по вопросам обработки ПД.

5.3. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений

5.3.1. Без письменного согласия субъекта ПД Клиника не раскрывает третьим лицам и не распространяет ПД, если иное не предусмотрено федеральным законом.

5.3.2. Запрещено раскрывать и распространять ПД субъектов ПД по телефону.

5.3.3. С целью защиты ПД в Клинике приказами директора назначаются (утверждаются):

- работник, ответственный за организацию обработки ПД;
- перечень должностей, при замещении которых обрабатываются ПД;
- перечень ПД, к которым имеют доступ работники, занимающие должности, предусматривающие обработку ПД;
- порядок доступа в помещения, в которых ведется обработка ПД;
- порядок передачи ПД в пределах Клиники;
- форма согласия на обработку ПД, форма согласия на обработку ПД, разрешенных субъектом персональных данных для распространения;
- порядок защиты ПД при их обработке в информационных системах ПД;
- порядок проведения внутренних расследований, проверок;

- иные локальные нормативные акты, принятые в соответствии с требованиями законодательства в области ПД.

5.3.4. Работники Клиники, которые занимают должности, предусматривающие обработку ПД, допускаются к ней после подписания обязательства об их неразглашении.

5.3.5. Материальные носители ПД хранятся в шкафах, запирающихся на ключ. Помещения Клиники, в которых они размещаются, оборудуются запирающими устройствами. Выдача ключей от шкафов и помещений осуществляется под подпись.

5.3.6. Доступ к персональной информации, содержащейся в информационных системах Клиники, осуществляется по индивидуальным паролям.

5.3.7. В Клинике используется сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.3.8. Работники Клиники, обрабатывающие ПД, периодически проходят обучение требованиям законодательства в области ПД.

5.3.9. В должностные инструкции работников Клиники, обрабатывающих ПД, включаются, в частности, положения о необходимости сообщать о любых случаях несанкционированного доступа к ПД.

5.3.10. В Клинике проводятся внутренние расследования в следующих ситуациях:

- при неправомерной или случайной передаче (предоставлении, распространении, доступе) ПД, повлекшей нарушение прав субъектов ПД;
- в иных случаях, предусмотренных законодательством в области ПД.

5.3.11. Работник, ответственный за организацию обработки ПД, осуществляет внутренний контроль:

- за соблюдением работниками, уполномоченными на обработку ПД, требований законодательства в области ПД, локальных нормативных актов;
- соответствием указанных актов требованиям законодательства в области ПД.

Внутренний контроль проходит в виде внутренних проверок.

5.3.12. Внутренние плановые проверки осуществляются на основании приказа директора Клиники.

5.3.13. Внутренние внеплановые проверки осуществляются по решению работника, ответственного за организацию обработки ПД. Основанием для них служит информация о нарушении законодательства в области ПД, поступившая в устном или письменном виде.

5.3.14. По итогам внутренней проверки оформляется докладная записка на имя руководителя Организации. Если выявлены нарушения, в документе приводится перечень мероприятий по их устранению и соответствующие сроки.

5.3.15. Внутреннее расследование проводится, если выявлен факт неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав субъектов ПД (далее – инцидент).

5.3.16. В случае инцидента Клиника в течение 24 часов уведомляет Роскомнадзор:

- об инциденте;
- его предполагаемых причинах и вреде, причиненном правам субъекта (нескольким субъектам) ПД;
- принятых мерах по устранению последствий инцидента;
- представителе Клинике, который уполномочен взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

При направлении уведомления нужно руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 № 187.

5.3.17. В течение 72 часов Клиника обязана сделать следующее:

- уведомить Роскомнадзор о результатах внутреннего расследования;
- предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

При направлении уведомления также необходимо руководствоваться Порядком и условиями взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и

массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных, утвержденными приказом Роскомнадзора от 14.11.2022 № 187.
5.3.18. В случае предоставления субъектом ПД (его представителем) подтвержденной информации о том, что ПД являются неполными, неточными или неактуальными, в них вносятся изменения в течение не позднее 3-х рабочих дней п.10 №187 Клиника уведомляет в письменном виде субъекта ПД (его представителя) о внесенных изменениях и сообщает (по электронной почте) о них третьим лицам, которым были переданы ПД.
5.3.19. Клиника уведомляет субъекта ПД (его представителя) об устранении нарушений в части неправомерной обработки ПД. Уведомляется также Роскомнадзор, если он направил обращение субъекта ПД (его представителя) либо сам сделал запрос.
5.3.20. В случае уничтожения ПД, которые обрабатывались неправомерно, уведомление направляется в соответствии с пунктом 5.3.19 настоящей Политики.
5.3.21. В случае уничтожения персональных данных, незаконно полученных или не являющихся необходимыми для заявленной цели обработки, Клиника уведомляет субъекта персональных данных (его представителя) о принятых мерах в письменном виде. Клиника уведомляет по электронной почте также третьих лиц, которым были переданы такие персональные данные.

6. Права субъекта ПД

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

- подтверждение факта обработки ПД оператором;
- правовые основания и цели обработки ПД;
- цели и применяемые оператором способы обработки ПД;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПД или которым могут быть раскрыты ПД 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, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ;
- 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 Федеральным законом от 27.07.2006 № 152-ФЗ или другими федеральными законами.

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

7. Обязанности Клиники

7.1. Клиника обязана:

- при сборе ПД предоставить информацию субъекту 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;
• не сообщать персональные данные субъекта ПД третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;
• не сообщать персональные данные субъекта ПД в коммерческих целях без его письменного согласия;
• предупредить лиц, получающих ПД субъекта ПД, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено;
• разрешать доступ к персональным данным субъекта ПД только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПД субъекта ПД, которые необходимы для выполнения конкретных функций.

8. Ответственность за нарушение норм, регулирующих обработку и защиту ПД

8.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных Контрагентов, а также в неправомерном разглашении информации, доступ к которой ограничен федеральным законом, причинении гражданину морального (физические или нравственные страдания) неправомерными действиями, нарушающими его личные неимущественные права либо посягающими принадлежащие гражданину другие нематериальные блага, а также в иных случаях, предусмотренных законом – могут быть привлечены к дисциплинарной, гражданско- правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством РФ.
8.2. Моральный вред, причиненный субъекту ПД вследствие нарушения его прав, нарушения правил обработки ПД, а также несоблюдения требований к их защите, установленных Федеральным законом от 27.07.2006 № 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПД убытков.

9. Заключительные положения

9.1. Положение вступает в действие с момента его утверждения приказом директора Клиники и обязательно для исполнения всеми работниками Клиники, имеющими доступ к персональным данным работников.
9.2. Во всех случаях, не предусмотренных настоящим Положением, следует руководствоваться действующим законодательством Российской Федерации.
9.3. Все изменения и дополнения к настоящему Положению утверждаются приказом директора Клиники.
9.4. Учреждение во исполнение требований п. 2, ст. 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» для обеспечения неограниченного доступа к сведениям о реализуемых Учреждением мероприятиях по защите персональных данных, и к документам, определяющим политику Клиники в отношении обработки персональных данных, размещает текст настоящего Положения на своем общедоступном официальном сайте в телекоммуникационной сети Интернет.