

Политика обработки персональных данных в медицинской организации

1. Общие положения

1.1. Настоящая Политика определяет порядок обработки персональных данных, в том числе данных пользователей веб-сайта, и меры по обеспечению безопасности персональных данных в ООО «МДЦ» (далее — Организация) 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 «МДЦ» и разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 21.07.2014г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно телекоммуникационных сетях» 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».

1.3. Настоящая Политика раскрывает принципы, порядок и условия обработки персональных данных физических лиц при обращении за медицинской помощью в медицинскую организацию.

Принципы, порядок и условия обработки ПДн кадрового состава клиники, а также ПДн, обрабатываемых в процессе исполнения договорных обязательств в процессе повседневной деятельности, в настоящей Политике не рассматриваются и регламентируются внутренними нормативными документами медицинской организации.

1.4. Основные понятия, используемые в Политике:

- Персональные данные. Любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
- Оператор персональных данных (оператор). Учреждение, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- Обработка персональных данных. Любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;
- Автоматизированная обработка персональных данных. Обработка персональных данных с помощью средств вычислительной техники
- 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 становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных; – обезличивание персональных данных. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- Информационная система персональных данных. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- Трансграничная передача персональных данных. Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- Субъект персональных данных. Физическое лицо, данные которого обрабатываются;
- Конфиденциальность персональных данных. Обязательное для оператора и иных лиц, получивших доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

1.5. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией 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.

1.6. Организация 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.

1.7 Действующая редакция хранится в месте нахождения Учреждения по адресу: г.Великий Новгород, ул. Дворцовая д.15 офис1, электронная версия Политики — на сайте по адресу: <https://mrkt-nov.ru/>.

1.8. Персональные данные обрабатывают с использованием средств автоматизации или без них.

2. Объём и категории обрабатываемых персональных данных

2.1. Пациенты, законные представители пациентов.

2.1.1. Персональные данные пациентов (лиц, являющихся стороной договора на оказание медицинских услуг), которые подлежат обработке:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата и место рождения;
- адреса места жительства и регистрации;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его орган;
- данные страхового свидетельства государственного пенсионного страхования;
- гражданство;
- информация о состоянии здоровья, наличии или отсутствии заболеваний, перечисленных в анкете о здоровье пациента, оформляемой в процессе сбора анамнеза.;
- семейное и социальное положение;
- контактный телефон; – адрес электронной почты;
- реквизиты полиса обязательного медицинского страхования;
- реквизиты полиса (договора) добровольного медицинского страхования;
- тип занятости;
- место работы;
- должность.

2.1.2 Список персональных данных, которые обрабатывает оператор на сайте медицинской организации - <https://mrkt-nov.ru/>: имя, номер телефона .

2.1.3. Кроме того, на сайте происходит сбор и обработка обезличенных данных о посетителях (в т.ч. файлов «cookie») с помощью сервисов интернет-статистики (Яндекс Метрика).

2.2. Перечень формируемых документов при обращении пациента в медицинскую организацию предусматривается Гражданским кодексом, Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», постановлением Правительства РФ от 11.05.2023 № 736 «Об утверждении правил предоставления медицинскими организациями платных медицинских услуг», приказом МЗ РФ от 14.09.2020 № 972н «Об утверждении порядка выдачи медицинскими организациями справок и медицинских заключений».

3. Цели и сроки обработки персональных данных

3.1. Оператор обрабатывает персональные данные в целях:

- исполнение договора на оказание медицинских услуг, стороной которого является пациент;
- медико-профилактические цели (установление медицинского диагноза, оказание медицинских услуг, контроль качества оказания медицинской помощи и др.).
- оказания медицинских услуг, в том числе идентификации пациентов (заказчиков), отражения информации в медицинской документации, предоставления сведений страховым компаниям (в случае оплаты ими оказываемых услуг), предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;
- выполнения требований действующего законодательства;

3.2. Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.3. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.5. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.6. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.7. Сроки обработки персональных данных напрямую зависят от сроков хранения гражданско-правовых договоров и медицинской документации и составляют:

- для персональных данных, полученных в связи с заключением договора на оказание медицинских услуг, – 5 лет;
- для персональных данных специальных категорий (данные о здоровье) – 25 лет в медицинской организации, 75 лет – в архиве.

4. Принципы и условия обработки персональных данных

4.1. Обработка персональных данных в ООО «МДЦ» производится на основе следующих принципов:

- законности и справедливости целей и способов обработки;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки избыточных персональных данных по отношению к заявленным целям их обработки;
- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей.

4.2. Медицинская организация обрабатывает персональные данные только при наличии хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных законом (подп. 4 п. 2 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ);
- обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных;
- производится обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (общедоступные данные);
- обрабатываются персональные данные, подлежащие опубликованию или обязательному раскрытию в соответствии с федеральным законом;
- обработка персональных данных производится в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

4.3. Медицинская организация и иные лица, получившие доступ к персональным данным в силу трудовых обязанностей, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5. Права субъекта персональных данных

5.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе без принуждения или введения в заблуждение с чьей-либо стороны.

5.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами.

5.3. Субъект персональных данных вправе требовать 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.

5.4. Запрещается принимать на основании исключительно автоматизированной обработки персональных данных решения, порождающие юридические последствия в отношении субъекта персональных данных или иным образом затрагивающие его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

5.5. Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

6. Права и обязанности Оператора

6.1. Отстаивать свои интересы в суде;

6.2. Предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

6.3. Отказывать в предоставлении персональных данных в случаях предусмотренных законодательством;

6.4. Использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством.

7. Обеспечение безопасности персональных данных

7.1. Безопасность персональных данных, обрабатываемых медицинской организацией, обеспечивается реализацией правовых, организационных, технических и программных мер, необходимых и достаточных для обеспечения требований федерального законодательства в области защиты персональных данных.

7.2. Основной задачей обеспечения безопасности ПДн при их обработке в Организации 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.

7.3. Меры по обеспечению безопасности персональных данных включают в себя, в частности:

- назначение ответственного за организацию обработки персональных данных;
- издание локальных правовых актов, регулирующих права и обязанности оператора персональных данных, описывающих систему мер по защите персональных данных, определяющих доступ к информационным системам персональных данных;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применение методов (способов) защиты информации;
- оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

7.4. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в

7.5. Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.

8. Заключительные положения

8.1. Настоящая Политика является локальным правовым актом, общедоступна и подлежит размещению на официальном сайте медицинской организации.

8.2. Контроль исполнения требований настоящей Политики осуществляется лицом, ответственным за организацию обработки персональных данных.