МЕДИЦИНА
medical center

ПРИКАЗ

24 ноября 2023г. **№ 40**

«О мерах по организации системы обработки персональных данных в ООО «Медицина»

В целях совершенствования порядка и системы защиты и обработки персональных данных, усиления контроля за соблюдением законодательства о персональных данных, норм и положений Конституции РФ, Трудового Кодекса РФ, Федерального закона от 27.07.2006г. № 152- ФЗ «О персональных данных», Федерального закона от 27.07.2006г. № 149- ФЗ «Об информации, информационных технологиях и защите информации», Федерального законаот 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
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», иных нормативных актов в сфере защиты персональных данных

ПРИКАЗЫВАЮ:

1. Приказ № 15 от 15.03.2015 отменить с даты издания настоящего приказа.

2. Утвердить:

2.1. ПОЛИТИКУ В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ООО «МЕДИЦИНА» (Приложение № 1)

2.2. ОБРАЗЕЦ СОГЛАСИЯ ПАЦИЕНТА/ЕГО ПРЕДСТАВИТЕЛЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ (Приложение № 2)
2.4. ОБРАЗЕЦ СОГЛАСИЯ РАБОТНИКА НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ (Приложение № 3)
2.5. ОБРАЗЕЦ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ КАНДИДАТА НА РАБОТУ (приложение 4)
2.6. ПОЛИТИКУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ САЙТА (Приложение №5)

3. Утвердить состав комиссии по уничтожению носителей, содержащих персональные данные (Приложение № 6)
4. Лицом ответственным за обработку персональных данных (ПДн), которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением организацией и его работниками требований действующего законодательства в области защиты и обработки ПДн является директор клиники, или лицо, временно его замещающее на основании приказа.
5. Приказ довести до сведения всех заинтересованных лиц клиники.
6. Контроль исполнения приказа оставляю за собой.

Директор
ООО «Медицина» **Незнамова И.В.**

Приложение № 1 к Приказу № 40 от 24.11.2023.
Утверждено и введено в действие
Приказом Директора ООО «Медицина»
№ 40 от 24.11.2023 г.
Незнамовой И.В.

ПОЛИТИКА
В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ООО «МЕДИЦИНА»

1. Общие положения

1.1. Настоящая политика клиники «Медицина» (далее -Клиника) в отношении обработки персональных данных (далее -политика) разработана в соответствии со ст. 10, ст. 18.1 Федерального закона от 27.07.2006г. № 152- ФЗ «О персональных данных», Конституцией РФ, Трудовым Кодексом РФ, Федеральным законом от 27.07.2006г. № 149- ФЗ «Об информации, информационных технологиях и защите информации», Постановлением Правительства РФ от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными действующими нормативными актами РФ и определяет позицию и намерения Клиники в области обработки и защиты персональных данных, соблюдения прав и основных свобод каждого гражданина.

1.2. Политика разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки персональных данных (далее –ПДн), направленного на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн, в том числе защиты права на неприкосновенность частной жизни, личную семейную тайну, врачебную тайну, в частности в целях защиты от несанкционированного доступа и неправомерного распространения ПДн, обрабатываемых в информационных системах Клиники.

1.3. Политика предназначена для изучения и неукоснительного соблюдения, исполнения всеми работниками клиники, и подлежит доведению до сведения, лицам состоящим в гражданско-правовых, трудовых и договорных отношениях с клиникой и других заинтересованных сторон.

1.4. Положения Политики распространяются на отношения по обработке и защите ПДн, полученной Клиникой как до, так и после утверждения настоящей Политики, за исключением случаев, когда по причинам правового, организационного или иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, 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 официальном сайте Организации, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения по адресу: город Пермь, Шоссе Космонавтов, 141, помещ. Офиса 2, информационный стенд, электронная версия Политики – на сайте по адресам в сети интернет: https://medicina-center.ru/

1.7. Контроль за исполнением требований настоящей Политики осуществляется уполномоченным лицом, назначенным ответственным за организацию обработки персональных данных.

2.Основные понятия

2.1.Обработка ПДн в клинике осуществляется в связи с исполнением законодательно возложенных на Клинику функций, определенных

- ✓ Трудовым Кодексом РФ
- ✓ Гражданским Кодексом РФ
- ✓ Налоговым Кодексом РФ
- ✓ Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»,
- ✓ Федеральным законом РФ от 07.02.1992 N 2300-1 "О защите прав потребителей"

✓ Федеральным законом № 152-ФЗ от 27.07.2006г. «О персональных данных»,

✓ Постановлением Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

✓ Постановлением Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

✓ Постановлением Правительства РФ от 11 мая 2023 г. N 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. N 1006»

✓ иными нормативными актами РФ, Уставом ООО «Медицина», договорами на оказание платных медицинских услуг, которые в совокупности являются **правовыми основаниями для обработки ПДн**.

Перечень ПДн, подлежащих защите формируется в соответствии с федеральным законодательством о ПДн.

2.2. Для целей настоящей Политики используются следующие понятия:

Персональные данные (ПДн) – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (гражданину).

К такой информации в частности относится:

ФИО, год, месяц, дата и место рождения, адрес, сведения о семейном, социальном, имущественном положении, сведения об образовании, профессии, доходах, стаже работы, предыдущих местах работы, биометрические данные, а также другая информация о физическом лице, включая биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фото/видео изображения, отпечатки пальцев, образ сетчатки глаза, особенности строения тела.

Обработка ПДн - любое действие (операция) или совокупность действий, операций с ПДу, совершаемых с использованием средств автоматизации или без использования таких средств. К таким действиям/операциям относятся сбор, извлечение, систематизация, накопление, хранение, уточнение (обновление, изменения), запись, передача (распространение, предоставление доступа), обезличивание, блокирование, удаление, уничтожение ПДн.

Оператор ПДн –государственный орган, муниципальный орган, юридического лицо, физическое лицо, организующее или осуществляющее обработку ПДн, а также определяющие цели и содержание обработки ПДн, состав ПДн, подлежащих обработке, действия (операции) совершаемые с ПД.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Передача 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;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Информационная система ПДн (ИСПДн) -совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Безопасность ПДн – защищенность ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

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 возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

3.Основные права и обязанности клиники, как оператора ПДн и субъекта ПДн.

3.1. Клиника имеет право:

- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Законом о персональных данных или другими федеральными законами;
- поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению клиники, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных;
- в случае отзыва субъектом персональных данных согласия на обработку персональных данных Клиника вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в Законе о персональных данных.

3.2. Клиника обязана:

✓ организовывать обработку персональных данных в соответствии с требованиями Закона о персональных данных;

✓ отвечать на обращения и запросы субъектов персональных данных и их законных представителей в соответствии с требованиями Закона о персональных данных;

✓ сообщать в уполномоченный орган по защите прав субъектов персональных данных (Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) по запросу этого органа необходимую информацию в течение 10 рабочих дней с даты получения такого запроса. Данный срок может быть продлен, но не более чем на пять рабочих дней, при наличии мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации;

✓ в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, включая информирование его о инцидентах, которые повлекли неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3.3. Субъект персональных данных имеет право:

✓ безвозмездно получать информацию, касающуюся обработки его персональных данных, за исключением случаев, предусмотренных федеральными законами. Сведения предоставляются субъекту персональных данных Клиникой в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных. Перечень информации и порядок ее получения установлен Законом о персональных данных

✓ получать от Клиники информацию о лицах, которые имеют доступ к ПДн субъекта, или которым может быть предоставлен такой доступ, о перечне обрабатываемых ПДн и источнике их получения, о сроках обработки персональных данных, в том числе сроки их хранения; получать сведения о том, какие юридические последствия для субъекта ПДн может повлечь за собой обработка его персональных данных

✓ получить доступ к ПДн, относящимся к ним специальным медицинским данным с помощью медицинского специалиста по выбору

✓ требовать от Клиники 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;

✓ дать предварительное согласие на обработку ПДн в целях заявленных для обработки ПДн

✓ отозвать свое согласие на обработку ПДн, сделав такое заявление в письменной форме, с указанием причин отзыва

✓ обжаловать в Роскомнадзоре или в судебном порядке неправомерные действия или бездействие Клиники при обработке его персональных данных.

4. Принципы обеспечения безопасности персональных данных

4.1. Основной задачей обеспечения безопасности ПДн при их обработке в Клинике 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.

4.2. Для обеспечения безопасности ПДн Клиника руководствуется следующими принципами:

–законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;

– **системность**: обработка ПДн 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;

– **комплексность:** защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Клиники и других имеющихся в Клиники 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 Клинике с учетом выявления новых способов и средств реализации угроз безопасности ПДн, актуального опыта в сфере защиты информации;

– **персональная ответственность:** ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД;

– **минимизация прав доступа:** доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

– **гибкость**: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых ПДн;

– **специализация и профессионализм**: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

– **эффективность процедур отбора кадров:** кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

– **наблюдаемость и прозрачность:** меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

– **непрерывность контроля и оценки:** устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

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

4.4. При обработке ПДн 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 ПДн.

5. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

5.1. Обработка персональных данных ограничивается **достижением конкретных, заранее определенных и законных целей.** Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5.2 **Цели обработки ПДн:**

- **для целей фактически осуществляемой Клиникой деятельности**: обеспечения организации оказания медицинской помощи населению, в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, ведения учета и систематизации оказанных услуг, в целях улучшения качества обслуживания пациентов, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 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», Закона РФ от 07.02.1992 N 2300-1 "О защите прав потребителей", Постановления Правительства РФ от 11 мая 2023 г. N 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. N 1006», Уставом ООО «Медицина»

- **для целей осуществление трудовых отношений**: исполнение трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, в том числе: содействие кандидатам в трудоустройстве, привлечение и отбор кандидатов на работу, получении дополнительного профессионального образования и повышения квалификации, прохождения аттестации, обеспечение личной безопасности работников, контроль количества и качества выполняемой работы, обеспечение сохранности имущества, ведение кадрового и бухучета, заполнение и передача в уполномоченные органы требуемых форм отчетности, организация постановки на индивидуальный (персонифицированный) учет работников в системах обязательного пенсионного страхования и обязательного социального страхования, осуществления пропускного режима;

- **для целей осуществления своей хозяйственной деятельности в соответствии с уставом ООО "Медицина",** в том числе заключение и исполнение договоров с контрагентами, формирования приходно-расходных, учетных документов по хозяйственным операциям, обеспечения пропускного режима, иных действий необходимых для исполнения обязательств по гражданско-правовым отношениям.

5.3. **Объем и категории обрабатываемых персональных данных.**

5.3.1.В клинике обрабатываются ПДн следующих субъектов:

– физические лица, являющиеся кандидатами на работу;

- физические лица, состоящие с клиникой в трудовых отношениях и физические лица, уволившиеся из учреждения;

– физические лица, являющие близкими родственниками сотрудников клиники;

— физические лица, состоящие с клиникой в гражданско-правовых отношениях;

– физические лица, обратившиеся в клинику за медицинской помощью, включая пользователей сайта

5.3.2. Объемы, обрабатываемых ПДн по каждой категории:

- **физические лица, являющиеся кандидатами на работу** - для целей отбора кандидатов, содействия в трудоустройстве, исполнения норм трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- контактные данные (телефон, адрес электронной почты)
- адрес места жительства;
- сведения об образовании, опыте работы, квалификации;
- сведения об инвалидности
- сведения о судимости
- иные персональные данные, сообщаемые кандидатами в резюме и сопроводительных письмах.

- физические лица, состоящие с клиникой в трудовых отношениях и физические лица, уволившиеся из учреждения:- для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений, осуществления пропускного режима:

- фамилия, имя, отчество;
- пол;
- гражданство;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства;
- адрес фактического проживания;
- контактные данные, номер телефона и адрес электронной почты;
- индивидуальный номер налогоплательщика;
- страховой номер индивидуального лицевого счета (СНИЛС);

- сведения об образовании, квалификации, профессиональной подготовке и повышении квалификации;
- фото/видео изображение;
- семейное положение, наличие детей, родственные связи;
- сведения о трудовой деятельности, в том числе наличие поощрений, награждений и (или) дисциплинарных взысканий;
- данные о регистрации брака;
- сведения о воинском учете;
- сведения об инвалидности;
- сведения об удержании алиментов;
- сведения о судимости
- сведения о доходе с предыдущего места работы;
- сведения о трудовом стаже, видах и периодах отпуска, временной нетрудоспособности, командировании, рабочем времени
- иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового законодательства.

- физические лица, являющие близкими родственниками сотрудников клиники- для целей исполнения трудового законодательства в рамках трудовых и иных непосредственно связанных с ним отношений:

- фамилия, имя, отчество;
- степень родства и пол;
- дата, месяц, год рождения и место;
- иные персональные данные, предоставляемые работниками в соответствии с требованиями трудового или налогового законодательства.

- физические лица, состоящие с клиникой в гражданско-правовых отношениях, либо представители юридических лиц контрагентов клиники

- фамилия, имя, отчество;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства;
- контактные данные (телефон, адрес электронной почты);
- занимаемая должность;
- индивидуальный номер налогоплательщика и СНИЛС;
- банковские реквизиты для расчетов;
- данные о применении специальных налоговых режимов;

- иные персональные данные, предоставляемые клиентами и контрагентами (физическими лицами), необходимые для заключения и исполнения договоров

- физические лица, обратившиеся в клинику за медицинской помощью – в целях обеспечения организации оказания медицинской помощи населению, в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, ведения учета и систематизации оказанных услуг, в целях улучшения качества обслуживания пациентов

- фамилия, имя, отчество
- пол и дата рождения,
- адрес места регистрации и места жительства
- паспортные данные,
- контактный(е) телефон(ы) и адрес электронной почты
- данные СНИЛС и ИНН
- данные о месте работы и занимаемой должности
- данные о состоянии здоровья, перенесенных заболеваниях,
- случаях обращения за медицинской помощью
- данные об инвалидности
- данные о результатах экспертизы нетрудоспособности
- данные о проведенных исследованиях и их результатах
- предварительный и окончательный диагноз
- биометрические данные, которые характеризуют физиологические и биологические особенности человека, включая данные рентгенологических и компьютерных исследований,
- данные функциональной диагностики, лабораторной диагностики,
- национальная принадлежность
- данные страхового полиса ОМС/ДМС,
- иные данные содержащиеся в амбулаторной карте больного, а также в иных документах, сопровождающих оказание платных медицинских услуг

- физические лица, пользователи сайта под доменным именем www.medicina-center.ru - целях идентификация пользователя, предоставление пользователю доступа к сервисам, информации и/или материалам, содержащимся на веб-сайте в информационных и медико-профилактических целях, поддержания связи с пользователем, получения запросов и информации, направленных на оказание медицинских услуг

- Обязательная для предоставления сервисов сайта информация помечена специальным образом (знаком «*» и предупреждением об обязательности предоставления информации:
- Фамилия, имя, отчество пользователя;
- Электронный адрес пользователя,
- Номер телефона пользователя.

Иная информация предоставляется пользователем на его усмотрение.

- данные, которые автоматически передаются сервисам сайта в процессе их использования с помощью установленного на устройстве пользователя программного обеспечения, в том числе IP-адрес, информация из cookie, информация о браузере пользователя (или иной программе, с помощью которой осуществляется доступ к сервисам), время доступа, адрес запрашиваемой страницы.
- иная информация о пользователе, сбор и/или предоставление которой необходимо для использования сервисов сайта.

5.3.3. Клиника осуществляет обработку **специальных категорий персональных данных**: национальная принадлежность, сведения о состоянии здоровья и интимной жизни, поскольку их обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, либо жизни, здоровья или иных жизненно важных интересов других лиц, при условии, осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что **обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну** и при условии что субъект дал согласие в письменной форме на обработку своих ПДн либо они являются общедоступными;

5.3.4. Клиникой **не осуществляется обработка специальных категорий** персональных данных, касающихся расовой принадлежности, политических взглядов, религиозных или философских убеждений, за исключением случаев, предусмотренных законодательством РФ.

6.Порядок и условия обработки персональных данных (получение, хранение, передача, ответы на запросы по ПДн, блокировка, уничтожение)

6.1. Обработка персональных данных осуществляется Клиникой в соответствии с требованиями законодательства Российской Федерации.

6.2. **Получение** персональных данных осуществляется с письменного согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

6.3. Если персональные данные возможно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Клиника должна сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта представить письменное согласие на их получение.

6.4. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в письменной форме дает его законный представитель.

6.5. В случае смерти субъекта согласие на обработку его персональных данных при необходимости дает в письменной форме один из его наследников, если такое согласие не было дано субъектом персональных данных при его жизни.

6.6. Клиника осуществляет обработку персональных данных для каждой цели их обработки следующими способами:

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

6.7. При получении ПДн, в том числе посредством информационно-телекоммуникационной сети Интернет, Клиника обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, **находящихся на территории Российской Федерации**

6.8. К обработке персональных данных допускаются работники Клиники, в должностные обязанности которых входит обработка персональных данных, согласно Схеме разграничения прав доступа сотрудников Оператора ПДн к категориям ПДн и объемам ПДн (Приложение №1), при условии принятия работником обязательств о неразглашении сведений конфиденциального характера и соблюдении режима конфиденциальности (Приложение №2).

6.9. Обработка персональных данных для каждой цели обработки, осуществляется путем:

- получения персональных данных в устной и письменной форме непосредственно от субъектов персональных данных,
- получения персональных данных посредством информационно-телекоммуникационной сети Интернет через защищенные каналы
- получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).
- копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);
- внесения персональных данных в журналы, учетные формы реестры и информационные системы Оператора;
- использования иных способов обработки персональных данных.

6.10. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения (согласие на размещение фотографии и видеоматериалов на сайте, в социальных медиа, иных СМИ и на информационных стендах ООО «Медицина» и т.д.), оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных по форме согласно Приказа Роскомнадзора от 24.02.2021 N 18. (по форме Приложение № 3)

6.11. Клиника **передает** ПДн третьим лицам в следующих случаях:

– субъект выразил свое согласие на такие действия;

– передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

6.12. Перечень лиц, которым передаются ПД

Третьи лица, которым передаются ПД:

– Пенсионный фонд РФ для учета (на законных основаниях);

– Налоговые органы РФ (на законных основаниях);

– Единый социальный фонд (на законных основаниях);

– Территориальный фонд обязательного медицинского страхования (на законных основаниях);

- Территориальный орган Роспотребнадзора и Центр «Гигиены и эпидеомиологии» по Пермскому краю

- Территориальный орган Росздравнадзора РФ

– страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);

– бухгалтерская организация для начисления заработной платы (на основании договора содержащего обязательства о неразглашении ПДн);

– судебные и правоохранительные органы в случаях, установленных законодательством;

- военный комиссариат;

– бюро кредитных историй (с согласия субъекта);

- органы МСЭ и лицензионные органы в сфере здравоохранения

- контрагенты и подрядчики на основании заключенных договоров (либо иных оснований) если в силу данных договоров они должны иметь доступ к персональным данным, только после подписания с ними обязательства о неразглашении сведений, содержащих персональные данные.

6.13. Ответы на правомерные письменные запросы предприятий, учреждений и организаций **даются с разрешения директора Клиники, в письменной форме** и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

6.14. **Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону**.

6.15. Клиника не осуществляет трансграничную передачу персональных данных.

6.16. Клиника осуществляет **хранение** персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требует каждая цель обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором.

6.17. ПДн субъектов могут передаваться на хранение как на бумажных носителях, так и в электронном виде. ПДн, зафиксированные на бумажных носителях, хранятся в несгораемых сейфах, запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа (регистратура, картотека и архив клиники).

6.18. ПДн на бумажных носителях хранятся в ООО "Медицина" в течение сроков хранения документов, для которых эти сроки предусмотрены законодательством об архивном деле в РФ (Федеральный закон от 22.10.2004 N 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 N 236)

6.19.ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

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

6.21. Срок хранения персональных данных, обрабатываемых в ИСПД, соответствует сроку хранения персональных данных на бумажных носителях.

6.22. Доступ к ПДн, сведения об фактах обработки ПДн, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Клиникой субъекту ПДн или его представителю **в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя**. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Клиника должна направить субъекту ПДн мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

6.23.В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

6.24.Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;
- подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Клиника предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

6.25.Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.26. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя либо по их запросу или по запросу Роскомнадзора Клиника осуществляет **блокирование** ПДн, относящихся к этому субъекту, с момента такого обращения или получения указанного запроса на период проверки, если блокирование не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.27.В случае подтверждения факта неточности персональных данных Клиника на основании сведений, представленных субъектом ПДн или его представителем, либо Роскомнадзором, или иных необходимых

документов **уточняет** ПДн в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.28. В случае выявления неправомерной обработки ПДн при обращении (запросе) субъекта персональных данных или его представителя, либо Роскомнадзора, Клиника осуществляет **блокирование** неправомерно обрабатываемых персональных данных, относящихся к этому субъекту, с момента такого обращения или получения запроса.

6.29. При выявлении Клиникой, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Клиника обязана:

- в течение 24 часов - уведомить Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставить сведения о лице, уполномоченном Клиникой на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;

- в срок, не превышающий трех рабочих дней с даты такого выявления, устранить допущенные нарушения

- в случае невозможности устранения допущенных нарушений Клинка в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязана **уничтожить персональные данные,** и уведомить об этом субъекта персональных данных

- в течение 72 часов - уведомить Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставить сведения о лицах, действия которых стали его причиной (при наличии).

6.30. Клиника **прекращает** обработку персональных данных в следующих случаях:

- если выявлен факт их неправомерной обработки - в течение 24 часов с выявления;

достигнута цель их обработки, ПДн подлежат уничтожению в соответствии со ст.21 №152-ФЗ от 27.07.2006, в течении тридцати дней, если иное не предусмотрено Законодательством Российской Федерации.

- истек срок действия или отозвано согласие субъекта ПДн на обработку указанных данных, когда по Закону о персональных данных обработка этих данных допускается только с согласия

6.31. В случае отзыва субъектом согласия на обработку своих ПДн Клиника обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением сторон и (или) федеральным законом. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

6.32. Материальные носители, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном законодательством об архивном деле в Российской Федерации.

Уничтожение носителей, содержащих ПДн производится путем сожжения, дробления (измельчения), превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

Электронные носители информации, и другие цифровые материалы, содержащие персональные данные по истечении срока их хранения уничтожаются путем стирания или форматирования носителя.

6.33. При уничтожении персональных данных, лица производящие отбор данных обязаны исключать возможность преждевременного их уничтожения.

6.34. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии (по форме согласно Приложению 4).

7. Защита персональных данных

7.1. В соответствии с требованиями нормативных документов в клинике создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

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

В клинике принимаются следующие меры правовой защиты ПДн

1) Приняты локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных; ведется оценка их актуальности;

2) назначено лицо, ответственное за обеспечение безопасности персональных данных

3) организуется обучение работников Клиники, осуществляющих обработку персональных данных. Допущенные к обработке ПД работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

4) проводится внутренний контроль и аудит

7.3. 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, рекламной деятельности, аналитической работы.

1) организована работа с информационными системами, в которых обрабатываются персональные данные

2) организовано хранение персональных данных в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

3) используются системы охранной сигнализации в помещениях клиники, с присвоением индивидуальных кодов доступа для каждого пользователя

4) обеспечивается хранение документации в несгораемом сейфе и картотеке под ключом, с доступом ограниченного круга лиц,

5) ограниченный доступ в локальной компьютерной сети, электронной почте

6) организуется восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

7.4. Подсистема **технической** защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

Основными мерами технической защиты ПДн, используемыми Организацией, являются:

1) определен актуальный уровень угрозы безопасности персональных данных при их обработке – 3 тип

2) при обработке персональных данных в информационных системах установлен 3 -й уровень защищенности

персональных данных.

3) обеспечена регистрация и учет всех действий, совершаемых с ПД в ИСПД;

4) установлены индивидуальные пароли доступа сотрудников в ИСПД в соответствии с их производственными обязанностями, ведется журнал регистрации их действий в ИС;

5) применяются средства защиты информации, учет машинных носителей ПД, обеспечение их сохранности; прошедших в установленном порядке процедуру оценки соответствия

6) используется лицензированное антивирусное программное обеспечение с регулярно обновляемыми базами;

7) используется лицензированное программное средство защиты информации от несанкционированного доступа;

8) используется SSL-сертификат который удостоверяет подлинность веб-сайта https://medicina-center.ru/

9) применяется ограничение доступа в локальной компьютерной сети, идентификация пользователей, с присвоением пароля доступа, регулярная смена паролей пользователей

10) изолирован сервер хранения баз данных,

11) организовано резервное копирование данных ИСПД, для предотвращения утери или сбоев в сети,

12) исключение возможности визуального считывания персональных данных с монитора посторонними лицами;

8. Заключительные положения

8.1.Иные права, обязанности, действия работников, в трудовые обязанности, которых входит обработка ПДн, определяются должностными инструкциями.

8.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

8.3. Разглашение персональных данных (передача их посторонним лицам, в том числе, работникам Клиники, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъектов, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим положением, локальными нормативными актами (приказами, распоряжениями), влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарной ответственности.

8.4. Работники Клиники, имеющие доступ к персональным данным субъектов, виновные в незаконном разглашении или использовании персональных данных без согласия из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии с Уголовным Кодексом Российской Федерации. Работники Клиники, имеющие доступ к персональным данным и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба Клинике, в соответствии с Трудовым Кодексом Российской Федерации.