УТВЕРЖДАЮ

Директор
ООО «Медицинский центр «Исток»

_____ В.И. Саттаров

«____» _____ 20__ г.

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ в ООО «МЕДИЦИНСКИЙ ЦЕНТР «ИСТОК»

г. Череповец

I. Порядок обработки персональный данных

1. Общие положения

1.1. Настоящее Положение о порядке обработки и защиты персональных данных (далее Положение) в ООО «Медицинский центр «Исток» (далее Учреждение) разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152–ФЗ «О персональных данных», Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ от 06.03.97 № 188, и иными нормативными актами, действующими на территории Российской Федерации.

1.2. Цель настоящего Положения – защита персональных данных от несанкционированного доступа и разглашения, неправомерного их использования или утраты.

1.3. Настоящим Положением регламентируется порядок сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения (далее обработка) персональных данных работников, кандидатов, контрагентов, несписочного состава и пациентов Учреждения (далее субъектов персональных данных).

1.4. Настоящее Положение вступает в силу с момента его утверждения руководителем учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным субъектов ПД.

1.5. Все дополнения и изменения к Положению утверждаются руководителем Учреждения.

1.6. Настоящее Положение доводится до сведения всех работников персонально под роспись.

2. Основные термины и определения

В настоящем Положении будут использоваться следующие термины и определения:

2.1. **Работник –** физическое лицо, состоящее в трудовых отношениях с Учреждением.

2.2. **Пациент** – физическое лицо, обратившееся за медицинской помощью или находящееся под медицинским наблюдением.

2.3. **Контрагент** – физическое или юридическое, являющееся одной из сторон договора в гражданско-правовых отношениях.

2.4. **Кандидат** – это физическое лицо, претендующее на вакансию.

2.5. **Несписочный состав** – это физические лица, оказывающие услуги (выполняющие работы) по договорам гражданско-правового характера, бывшие работники, ветераны, практиканты и пр.

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

2.7. **Субъект персональных данных –** лицо, к которому указанные ПД относятся.

2.8. **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПД, а также определяющие цели обработки ПД, состав ПД, подлежащих обработке, действия (операции), совершаемые с ПД.

2.9. **Обработка персональных данных –** любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПД.

2.10. **Автоматизированная обработка персональных данных** – обработка ПД с помощью средств вычислительной техники.

2.11. **Распространение персональных данных** – действия, направленные на раскрытие ПД неопределенному кругу лиц.

2.12. **Предоставление персональных данных** – действия, направленные на раскрытие ПД определенному лицу или определенному кругу лиц.
2.13. **Блокирование персональных данных** – временное прекращение обработки ПД (за исключением случаев, если обработка необходима для уточнения ПД).
2.14. **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание ПД в информационной системе ПД и (или) в результате которых уничтожаются материальные носители ПД.
2.15. **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПД конкретному субъекту ПД.
2.16. **Использование персональных данных –** это действие (операция) с ПД, совершаемые получившим доступ к ним лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПД либо иным образом затрагивающих его права и свободы.
2.17. **Информационная система персональных данных** (далее ИС ПД) – это информационная система, представляющая собой совокупность ПД, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПД с использованием средств автоматизации или без использования таких средств.
2.18. **Архив персональных данных** (далее АПД) – это совокупности ПД, представленных не в электронном виде и хранящихся вне информационных систем, на бумажном или ином носителе, объединенных на основе критерия места хранения и цели обработки (бухгалтерия, кадровая и медицинская службы и т.п.).
2.19. **Конфиденциальная информация** – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.
2.20. **Конфиденциальность персональных данных** – обязательное для соблюдение оператором или иным получившим доступ к ПД лицом требование не допускать их распространения без согласия субъекта ПД или наличия иного законного основания.
2.21. **Защита персональных данных** – деятельность управомоченных лиц по обеспечению с помощью локального регулирования порядка обработки ПД и организационно-технических мер конфиденциальности информации о конкретном субъекте.
2.22. **Общедоступные персональные данные** – ПД, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяется требования соблюдения конфиденциальности.
2.23. **Доступ к информации** – возможность получения информации и ее использования.

3. Основные права субъектов персональных данных

Действующее законодательство предоставляет субъектам ПД следующие основные права:
3.1. Право на получение сведений об операторе (Учреждении), о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту ПД, а также на ознакомление с этими ПД.
3.2. Право на получение информации, касающейся обработки его ПД, в частности:
3.2.1. право знать, кто и в каких целях использует или использовал его ПД;
3.2.2. свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его ПД, за исключением случаев, предусмотренных федеральным законом.
3.3. Право на определение представителей для защиты своих ПД.
3.4. Право требовать исключить или исправить неверные или неполные ПД, а также данные, обработанные с нарушением требований настоящего Положения. При отказе оператора исключить или исправить ПД субъект имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия.
3.5. Право требовать от Учреждения извещения всех лиц, которым ранее были сообщены неверные или неполные его ПД, обо всех произведенных в них исключениях, исправлениях или дополнениях.
3.6. Вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по

защите прав субъектов ПД или в судебном порядке.

3.7. Право на сохранение и защиту своей личной и семейной тайны.

3.8. Право не предоставлять сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни, за исключением случаев, когда такие ПД являются общедоступными.

3.9. Субъект ПД имеет право принимать решение о предоставлении своих ПД оператору (Учреждению) или третьему лицу, дав оператору письменное согласие на их обработку.

4. Основные обязанности субъектов персональных данных

В целях обеспечения достоверности ПД субъект обязан:

4.1. Предоставить Учреждению или его представителю полные и достоверные данные о себе.

4.2. Своевременно сообщать Учреждению об изменении своих ПД.

5. Основные права оператора (Учреждения)

5.1. Учреждение может использовать автоматизированную обработку ПД и обработку ПД без использования средств автоматизации.

5.2. Учреждение может возлагать выполнение отдельных мероприятий по защите ПД, на сторонние организации (подрядчиков, исполнителей).

5.3. Учреждение может осуществлять обработку ПД, касающихся состояния здоровья, при выполнении одного из условий:

5.3.1. получено предварительное письменное согласие субъекта ПД на такую обработку;

5.3.2. обработка ПД 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;

5.3.3. ПД относятся к состоянию здоровья субъекта ПД и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

5.3.4. обработка ПД необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПД, а также для заключения договора по инициативе субъекта ПД или договора, по которому субъект ПД будет являться выгодоприобретателем или поручителем;

6. Основные обязанности оператора (Учреждения)

6.1. Строго соблюдать действующее законодательство о ПД и обеспечивать их конфиденциальность в соответствии с настоящим Положением.

6.2. Осуществлять защиту ПД субъектов.

6.3. Обеспечить хранение учетной документации содержащей сведения о ПД субъектов. При этом ПД не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

6.4. Заполнять документацию содержащую ПД субъекта в соответствии с установленными требованиями действующего законодательства и внутренними локальными актами Учреждения.

6.5. Субъекты и их представители должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки ПД, а также об их правах и обязанностях в этой области.

6.6. При определении объема и содержания, обрабатываемых ПД Учреждение должно руководствоваться Конституцией РФ, Трудовым кодексом РФ, Гражданским кодексом РФ и иными федеральными законами.

6.7. Вести учет передачи ПД субъектов третьим лицам путем ведения соответствующего журнала (Приложение № **1**), отражающего сведения о поступившем запросе (кто является

отправителем запроса, дата его поступления оператору, дату ответа на запрос, какая именно информация была передана либо отметку об отказе в ее предоставлении.

7. Порядок обработки Учреждением персональных данных

В целях обеспечения прав и свобод человека и гражданина Учреждение и его представители при обработке персональных данных субъектов обязаны соблюдать следующие общие требования:

7.1. **Сбор информации:**

7.1.1. Все ПД субъекта следует получать лично у субъекта ПД.

7.1.2. Если ПД возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (либо письменный отказ). Учреждение должно сообщить субъекту о целях, предполагаемых источниках и способах получения ПД, характере подлежащих получению ПД и последствиях отказа субъекта дать письменное согласие на их получение.

7.2. **Согласие субъекта персональных данных на обработку своих персональных данных:**

7.2.1. Согласие на обработку персональных данных – это документ, по которому субъект ПД дает свое согласие оператору ПД на обработку персональных данных (Приложение № **2** и **3**).

7.2.2. Письменное **согласие** субъекта ПД на обработку своих ПД **должно включать** в себя:

- фамилию, имя, отчество, адрес субъекта ПД, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес оператора (Учреждения);
- цели обработки ПД;
- перечень ПД, на обработку которых дается согласие субъекта ПД;
- перечень действий с ПД, на совершение которых дается согласие;
- общее описание используемых Учреждением способов обработки ПД;
- срок, в течение которого действует согласие, а также порядок его отзыва.

7.2.3. **Согласие** на обработку ПД **не требуется** в следующих случаях:

- обработка ПД осуществляется на основании федерального закона, устанавливающего ее цель, условия получения ПД и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка ПД осуществляется в целях исполнения договора, одной из сторон которого является субъект ПД;
- обработка ПД необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД, если получение согласия субъекта ПД невозможно;
- обработка ПД необходима в связи с осуществлением правосудия;
- в других, предусмотренных законодательством случаях.

7.2.4. В целях защиты частной жизни, личной и семейной тайны субъекты не должны отказываться от своего права на обработку ПД только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7.3. **Внесение персональных данных в общедоступные источники:**

7.3.1. С письменного согласия субъекта ПД к общедоступным ПД на период действия трудового договора могут быть отнесены следующие ПД: фамилия, имя, отчество, место работы, дата приема на работу, образование, подразделение, должность, координаты рабочего места, табельный номер, рабочий телефон, рабочий электронный адрес.

7.3.2. Общедоступные ПД могут быть размещены в общедоступных корпоративных источниках (справочниках Учреждения).

7.3.3. Установление режима конфиденциальности в отношении общедоступных ПД не требуется.

7.3.4. При прекращении правоотношений между Учреждением и субъектом ПД по любому основанию согласие субъекта ПД об отнесении указанных выше данных к общедоступным прекращает свое действие.

7.3.5. Информация по этому субъекту ПД, размещенная в общедоступных корпоративных справочниках, должна быть удалена.

7.4. **При передаче персональных данных, за исключением общедоступных, необходимо соблюдать следующие требования:**

7.4.1. Не сообщать ПД субъекта третьей стороне без его письменного согласия, за исключением случаев, установленных федеральным законом.
7.4.2. Не сообщать ПД субъекта в коммерческих целях без его письменного согласия.
7.4.3. Предупредить лиц, получающих ПД субъекта, 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. Лица, получающие ПД, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен ПД субъекта в порядке, установленном федеральными законами.
7.4.4. Передавать ПД только при условии принятия на себя лицами, их получающими от Учреждения, обязательства по охране конфиденциальности и соблюдению ограничений использования ПД и требовать от этих лиц подтверждения того, что указанные обязательства соблюдаются.
7.4.5. Разрешать доступ к ПД субъекта только специально уполномоченным лицам, определенным настоящим положением, при этом указанные лица должны иметь право получать только те ПД, которые необходимы для выполнения конкретных функций.
7.4.6. Передавать ПД субъекта его представителю в порядке, установленном законодательством, и ограничивать эту информацию только теми ПД, которые необходимы для выполнения указанными представителями их функций.
7.4.7. Передавать ПД от держателя или его представителей внешнему потребителю в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
7.4.8. Осуществлять передачу ПД субъекта в пределах Учреждения в соответствии с настоящим Положением.
7.4.9. Ни в каких случаях не допускается передача ПД, обрабатываемых Учреждением, способами, не позволяющими идентифицировать принимающего субъекта, в том числе по телефонному запросу.
7.5. **Защита персональных данных:**
7.5.1. Персональные данные относятся к конфиденциальной информации, то есть порядок работы с ними регламентирован действующим законодательством РФ и осуществляется с соблюдением строго определенных правил и условий.
7.5.2. Не требуется обеспечение конфиденциальности ПД:
- в случае обезличивания персональных данных;
- по истечении срока их хранения установленного законодательством РФ об архивном деле;
- в отношении общедоступных персональных данных.

7.5.3. Все меры конфиденциальности при сборе, обработке и хранении ПД субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
7.5.4. Хранение ПД должно происходить в порядке, исключающем их утрату или их неправомерное использование.
7.5.5. Под угрозой или опасностью утраты ПД понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.
7.5.6. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.
7.5.7. Защита ПД представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ПД и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.
7.5.8. Учреждение осуществляет следующие **основные мероприятия по защите персональных данных**:
- разграничение доступа к ПД;
- установление в отношении персональных данных режима конфиденциальности;

- возложение на работников и контрагентов, получающих ПД, обязательства по обеспечению их конфиденциальности;
- защита ПД в информационных системах посредством аппаратных и программных средств;
- ограничение доступа к серверам и рабочим станциям, с помощью которых возможно получить доступ к информационным системам, содержащим персональные данные;
- ограничение доступа в помещения, в которых ПД хранятся вне информационных систем (на бумажных и аналогичных носителях);
- хранение ПД в любом формате исключительно в охраняемых помещениях с соблюдением противопожарных и иных технических норм.

Внутренняя защита ПД

7.5.9. Основным виновником несанкционированного доступа к ПД является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами Учреждения.

7.5.10. Для обеспечения **внутренней защиты** ПД субъектов необходимо соблюдать ряд мер:

- ограничение и регламентация состава операторов (работников), функциональные обязанности которых требуют знания конфиденциальной информации;
- строгое избирательное и обоснованное распределение документов и информации между операторами;
- рациональное размещение рабочих мест операторов, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание оператором требований нормативно–методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава операторов, имеющих право доступа (входа) в помещение, в котором находятся носители конфиденциальной информации;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа операторами;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- все электронные базы данных и информационные системы содержащие ПД, должны быть защищены паролем, который сообщается операторам, имеющим доступ к ПД.

Внешняя защита ПД

7.5.11. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

7.5.12. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров, бухгалтерии, мед. службе и других подразделениях, обрабатывающих ПД.

7.5.13. Для обеспечения **внешней защиты** ПД необходимо:

- ограничение беспрепятственного доступа в помещения где хранятся и обрабатываются документы содержащие ПД;
- технические средства охраны;
- охрана территории, зданий и помещений;

– учет и контроль деятельности посетителей.

7.5.14. Защита ПД от неправомерного их использования или утраты должна быть обеспечена Учреждением за счет собственных средств в порядке, установленном действующим российским законодательством.

8. Доступ к персональным данным

8.1. Учреждение обеспечивает ограничение доступа к ПД субъектов лицам, не уполномоченным законом либо Учреждением для получения соответствующих сведений.

8.2. Неограниченный доступ ко всем ПД, обрабатываемым Учреждением, предоставляется директору Учреждения и его заместителю.

8.3. Директор Учреждения и его заместитель вправе своими приказами определить работников Учреждения, уполномоченных на предоставление допуска к ПД (далее «Лица со специальными полномочиями»).

8.4. Перечень должностей, которым предоставлен доступ к ПД приведен в приложении № **4**.

8.5. Лица, указанные в п. 8.2. и 8.3. Положения, вправе предоставлять доступ к ПД, обрабатываемым Учреждением, другим лицам, не указанным в Приложении № **4** путем выдачи допуска (Приложение № **5**).

8.6. Директор и его заместитель, а так же лица со специальными полномочиями принимают решение о допуске работников, неуказанных в Приложении № **4** к ПД субъектов в объеме, необходимом для выполнения своих должностных обязанностей (как они определены в соответствующих должностных инструкциях) и организуют учет сотрудников, допущенных к ПД.

8.7. Обязательными условиями доступа к ПД, обрабатываемым Учреждением, как для его работников, так и для его контрагентов, являются:

8.7.1. ознакомление под роспись с Перечнем обрабатываемых Учреждением ПД (Приложение № **6**) и с настоящим Положением;

8.7.2. принятие обязательства по обеспечению конфиденциальности ПД (Приложение № **7** и **8**); и соблюдения настоящего Положения.

8.8. При увольнении работника, имеющего доступ к обработке ПД, его учетная запись (права) должны быть заблокированы.

8.9. Лица со специальными полномочиями в объеме своих полномочий должны ежегодно организовывать проведение сверки по ролям и работникам, обрабатывающим ПД. Цель проверки – минимизация полномочий, а также выявление и блокирование учетных записей пользователей, которым доступ к обработке ПД не требуется.

9. Перечень персональных данных, обрабатываемых Учреждением

9.1. Перечень ПД, обрабатываемых Учреждением (Приложение № **6**), утверждается руководителем.

9.2. В Перечне указываются ПД по категориям граждан, чьи данные обрабатываются в Учреждении, и видам ПД.

9.3. По каждому виду персональных данных указывается: содержание персональных данных, категория, источник получения, основание для обработки, срок хранения и условия прекращения обработки ПД.

9.4. Непосредственно ПД в Перечень не включаются.

9.5. Перечень ПД работников и кандидатов ведет инспектор (специалист) по кадрам; пациентов - главная медицинская сестра; контрагентов и физических лиц – главный бухгалтер. Запрещается изменение Перечня без согласования с ответственными лицами.

9.6. Каждый работник Учреждения ознакамливается с перечнем ПД, обрабатываемых Учреждением, под роспись. (Приложение № **9**)

10. Реестр информационных систем персональных данных и архивов персональных данных

10.1. Уполномоченное приказом директора лицо ведет Реестр, в котором содержится информация обо всех имеющихся в Учреждении информационных системах персональных данных (далее – ИСПД). (см. форму реестра в Приложении № **10**).

10.2. Дополнительно в Реестр записывается информация об архивах персональных данных (далее – АПД).

10.3. В отношении каждой ИСПД /каждого АПД в Реестре указывается: наименование ИСПД/АПД, место нахождения ИСПД/АПД (адрес, помещение), общая характеристика субъектов, ПД которых хранятся в ИСПД/АПД (контрагенты, работники, пациенты, их отдельные категории и т.д.), общая характеристика ПД, хранящихся в ИСПД/АПД (реквизиты договоров, бухгалтерская информация, кадровая документация и т.д.), результат классификации ИСПД/АПД, подразделение, в интересах которого осуществляется ведение ИСПД/АПД (далее - «Заинтересованное подразделение»); лицо, ответственное за работу с ИСПД/АПД (назначенное приказом директора Учреждения), наличие/отсутствие в ИСПД/АПД специальных категорий ПД, указанных в п.3.8. и 5.3 настоящего положения.

10.4. Непосредственно ПД в Реестр не включаются.

10.5. Лица, ответственные за работу с ИСПД и АПД, обязаны незамедлительно информировать Уполномоченное лицо о любых известных изменениях, подлежащих отражению в Реестре. Уполномоченное лицо на регулярной основе запрашивает у указанных выше лиц информацию о текущих характеристиках ИСПД и АПД, необходимых для ведения Реестра.

10.6. Реестр ведется в электронном виде.

11. Обработка запросов субъектов персональных данных

11.1. Субъект ПД вправе требовать от оператора (Учреждения), путем оформления запроса:

11.1.1. получения сведений об Учреждении, о месте его нахождения;

11.1.2. получения сведений о наличии у Учреждения его ПД;

11.1.3. ознакомления со своими ПД;

11.1.4. уточнения своих ПД, их блокирования или уничтожения, если ПД являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

11.2. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПД, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта ПД или его законного представителя.

11.3. Запросы субъектов ПД (далее – «Запросы») направляются ответственному за ведение ИСПД и АПД не позднее следующего рабочего дня после их получения.

11.4. Ответственное лицо производит учет Запроса и в течение одного рабочего дня проверяет соответствие Запроса требованиям действующего законодательства (п.3 ст. 14 ФЗ «О персональных данных»). Если Запрос не соответствует требованиям действующего законодательства, то в течение трех рабочих дней с момента получения Запроса Учреждением готовит мотивированный письменный ответ за своей подписью и отправляет его лицу, направившему Запрос.

11.5. Если поступивший Запрос соответствует требованиям действующего законодательства и касается получения сведений о наличии у Учреждения его ПД, ознакомления с такими ПД, то в целях подготовки ответа:

- ответственное лицо выявляет список ИСПД/АПД в которых содержаться ПД субъекта и направляет внутренние запросы лицам, ответственным за работу с этими ИСПД/АПД;
- ответственные за работу с ИСПД/АПД в срок не более трех рабочих дней направляют ответы на указанные внутренние запросы.

11.6. На основании информации, полученной в соответствии с п. 11.3 настоящего положения, ответственное лицо готовит ответ на Запрос, который должен быть подписан от имени Учреждения работником, обладающим необходимыми полномочиями, и направлен заявителю (субъекту ПД) не позднее семи рабочих дней с момента получения Запроса Учреждением.

11.7. Если Запрос субъекта ПД соответствует требованиям действующего законодательства и касается корректировки своих ПД (в том случае, когда ПД являются неполными, устаревшими или недостоверными: изменения паспортных данных, состава семьи и т.п.), то такие Запросы сразу направляются на исполнение ответственному лицу.

11.8. Ответственное лицо хранит в течение 5 лет Запросы, ответы на них и иные доказательства направления таких ответов. При наличии в Запросе или у Учреждения почтового адреса лица, направившего Запрос, ответственное лицо обязано, направить ответ на Запрос заказным письмом и хранить доказательства такого направления. При возможности выдать ответ на Запрос под расписку (например – работникам Учреждения), ответ на Запрос выдается под расписку, подлежащую хранению ответвленным сотрудником.

11.9. При обращении субъектов ПД (их законных представителей) с устными требованиями: об ознакомлении с документацией непосредственно его касающейся, о получении копий такой документации, о получении справок, а равно при предоставлении субъектами документов и информации, направленной на корректировку их ПД, ознакомление субъектов со своими ПД, выдача соответствующих справок и корректировка ПД осуществляется в порядке, установленном директором Учреждения, в срок, не превышающий трех рабочих дней с момента соответствующего обращения. При этом производится идентификация личности обратившегося субъекта (его законного представителя) на основании удостоверяющих личность документов. При устном обращении законного представителя субъекта ПД также производится проверка его полномочий. Такие запросы Уполномоченным лицом учету не подлежат.

11.10. Запросы субъектов ПД, касающиеся получение сведений об операторе, о месте его нахождения; уточнения, блокирования или уничтожения ПД субъекта ПД, направившего Запрос, в случае, если его ПД являются, незаконно полученными, не являются необходимыми для заявленной цели обработки или в случае их неправомерного использования исполняются Уполномоченным лицом.

11.11. Если поступивший Запрос соответствует требованиям действующего законодательства, он обрабатывается в следующем порядке:

11.11.1. Уполномоченное лицо направляет внутренние запросы лицам, ответственным за работу с ИСПД/АПД, в которых могут содержаться ПД, подлежащие возможному уточнению, блокированию или уничтожению осуществляется в день получения Запроса. Ответ на указанный внутренний запрос информации направляется соответствующим ответственным лицом не позднее следующего рабочего дня за его получением.

11.11.2. Не позднее рабочего дня, следующего за днем получения ответа на внутренний запрос информации, уполномоченное лицо принимает решение о необходимости или отсутствии необходимости блокирования ПД. Решение об отсутствии необходимости блокирования ПД принимается при обнаружении достоверности ПД и очевидном отсутствии признаков их неправомерного использования. Решение о блокировании ПД принимается при обнаружении признаков недостоверности ПД или их неправомерного использования

11.11.3. При принятии решения о блокировании ПД *уполномоченное лицо* одновременно принимает решение о начале проверки факта недостоверности ПД или их неправомерного использования.

11.11.4. Проверка факта недостоверности ПД осуществляется руководителем заинтересованного подразделения, к которому относятся ИСПД/АПД, предположительно содержащие недостоверные данные, или уполномоченными им лицами (в случае наличия предположительно недостоверных ПД субъекта в ИСПД/АПД, относящихся к нескольким заинтересованным подразделениям, по совместному решению их руководителей, проверка проводится силами одного из таких подразделений). При проверке факта недостоверности ПД должны быть проверены документы, представленные субъектом ПД (его законным представителем) одновременно с Запросом, а также, при необходимости, у указанного субъекта и у иных лиц могут запрашиваться дополнительные документы и информация.

11.12. По результатам проверок, предусмотренных настоящим разделом положения, принимается одно из следующих решений:

11.12.1. при отсутствии фактов недостоверности/неправомерного использования ПД – об их разблокировании;

11.12.2. при обнаружении факта недостоверности ПД – об их изменении;

11.12.3. при обнаружении факта совершения неправомерных действий с ПД – об устранении допущенных нарушений в срок, не превышающий трех рабочих дней с даты такого выявления. В случае невозможности устранения допущенных нарушений – об уничтожении ПД в этот же срок.

Решения, принятые в соответствии с настоящим пунктом положения, должны быть в форме письменного ответа доведены до сведения лица, направившего Запрос. Указанный ответ должен быть направлен субъекту, направившему Запрос, способом, обеспечивающим наличие у Учреждения доказательств его направления и/или получения адресатом. Внутренние запросы информации и ответы на них, предусмотренные настоящим положением, могут направляться в электронной форме.

11.13. Запросы, ответы на них и доказательства направления таких ответов хранятся в учреждении в течение 5 лет. При возможности выдать ответ на Запрос под расписку (например – работникам Учреждения), ответ на Запрос выдается под расписку, подлежащую хранению.

II. Защита персональных данных в информационных системах персональных данных

1. Основные принципы защиты персональных данных в ИСПД

1.1. При обработке ПД в информационной системе Учреждение обеспечивает:

1.1.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;

1.1.2. своевременное обнаружение фактов несанкционированного доступа к ПД;

1.1.3. недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;

1.1.4. возможность незамедлительного восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

1.1.5. постоянный контроль обеспечения уровня защищенности ПД.

1.2. Мероприятия по обеспечению безопасности ПД при их обработке в ИС включают в себя:

1.2.1. определение угроз безопасности ПД при их обработке, формирование на их основе модели угроз;

1.2.2. разработку на основе модели угроз системы защиты ПД, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПД, предусмотренных для соответствующего класса ИС;

1.2.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

1.2.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

1.2.5. обучение лиц, использующих средства защиты информации, применяемые в ИС, правилам работы с ними;

1.2.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей ПД;

1.2.7. учет лиц, допущенных к работе с ПД в информационной системе;

1.2.8. контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

1.2.9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПД, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

1.2.10. описание системы защиты ПД.

1.3. Ответственным за организацию защиты ПД в ИСПД (включая организацию проведения выше перечисленных мероприятий, кроме п.п. 1.2.7 настоящей главы) лицо, назначаемое

приказом директора учреждения. Ответственность за реализацию мероприятий, предусмотренных п. 1.2.7. настоящей главы, возлагается на лиц, назначенных ответственными за работу с соответствующими ИСПД в порядке, установленном п.п. 10.3. главы I настоящего Положения.

2. Методы и способы защиты персональных данных в ИСПД

2.1. Для обеспечения защиты ПД при их обработке в ИСПД, в зависимости от разработанной для ИСПД модели угроз безопасности ПД, реализуются следующие методы:

2.1.1. защита от несанкционированного доступа и неправомерных действий к ПД при их обработке в ИСПД;

2.1.2. защита ПД от утечки по техническим каналам.

2.2. В состав способов защиты ПД при их обработке в ИСПД от несанкционированного доступа и неправомерных действий входят следующие способы:

2.2.1. защита от несанкционированного доступа при однопользовательском и многопользовательском режимах обработки ПД с различными правами доступа к ним;

2.2.2. защита ПД при межсетевом взаимодействии ИСПД;

2.2.3. защита от вредоносного программного обеспечения;

2.2.4. использование программных или программно-аппаратных средств (систем) обнаружения вторжений.

2.3. Кроме этого, в зависимости от разработанной для ИСПД модели угроз безопасности ПД, может проводиться контроль на наличие недекларированных возможностей в программном и программно-аппаратном обеспечении и анализ защищенности системного и прикладного программного обеспечения.

3. Действия в случае обнаружения нарушения правил использования ИСПД

3.1. Лицо, обнаружившее факт нарушения правил использования ИСПД (несанкционированные доступ, изменение ИСПД, несоблюдение условий хранения ПД и т.п.), обязано сообщить об этом своему непосредственному руководителю и Уполномоченному лиц).

3.2. По факту обращения, указанного в п.п.3.1., Уполномоченное лицо инициирует проверку, для проведения которой могут привлекаться любые необходимые специалисты Учреждения (юристы, специалисты по информационным технологиям и т.д.).

3.3. Проверка должна быть проведена и закончена в течение 10 рабочих дней с момента обнаружения факта нарушения правил пользования ИСПД.

3.4. Срок, предусмотренный п.п. 3.3, может быть продлен Уполномоченным лицом, но не более чем на 20 рабочих дней.

3.5. Результаты проверки должны быть оформлены в виде заключения, содержащего:

3.5.1. описание выявленных фактов нарушения правил пользования ИСПД;

3.5.2. выводы о причинах и условиях, приведших к допущенным нарушениям;

3.5.3. предложения о дальнейших действиях, связанных с выявленными нарушениями (инициирование юридических процедур, направленных на привлечение виновных лиц к ответственности и взыскании с них сумм причиненного ущерба, принятие мер по минимизации негативных последствий нарушения для субъектов ПД и Учреждения и т.п.);

3.5.4. предложения по устранению причин и условий, приведших к допущенным нарушениям (совершенствование ИСПД, изменение режима доступа к ней, пересмотр результатов классификации ИСПД и т.п.).

3.6. Результаты проверки должны быть доведены до сведения лица, ответственного за работу с ИСПД не позднее одного рабочего дня с момента их оформления. Доведение результатов проверки до сведения лица, обнаружившего факт нарушения правил пользования ИСПД, осуществляется исключительно по требованию такого лица и при условии, что при этом не разглашаются конфиденциальные сведения, доступ к которым у такого лица отсутствует.

III. Особенности обработки и защиты персональных данных в АПД

1. Основные способы защиты персональных данных в АПД

1.1. Лица, осуществляющие обработку ПД в АПД, наряду с соблюдением условий, установленных п. 8. главы I настоящего положения, должны быть проинформированы об особенностях и правилах такой обработки, установленных Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утверждены Постановлением Правительства РФ от 15 сентября 2008 г. № 687) (далее в настоящем разделе – «Правила»), иными нормативными актами Российской Федерации и настоящим положением.

1.2. Все АПД, имеющие различные цели обработки, должны храниться отдельно.

1.3. Доступ в помещения, в которых хранятся АПД, предоставляется исключительно лицам, имеющим допуск к соответствующим АПД (их частям). Указанные помещения должны находиться исключительно в охраняемых зданиях, запираться, при этом факт доступа в них должен, по возможности, фиксироваться (электронные системы, журналы выдачи ключей и т.п.).

1.4. Материальные носители, входящие в состав АПД и содержащие ПД, должны соответствовать п.п. 4,5,7,8, 9 и 11 Правил.

2. Хранение материальных носителей, содержащих персональные данные в составе АПД

2.1. В целях обеспечения сохранности ПД в составе АПД и исключения несанкционированного доступа к ним Учреждением приняты следующие меры:

2.1.1. ограничение и контроль доступа в помещения, в которых хранятся АПД;

2.1.2. осуществление обработки ПД в АПД способами, исключающими доступ к ним не уполномоченных лиц, в том числе посредством дистанционного наблюдения (запрет на вынос материальных носителей, содержащих ПД из мест их хранения, иные необходимые меры);

2.1.3. поддержание помещений, в которых хранятся АПД, в технически пригодном состоянии, в т.ч. в строгом соответствии с противопожарными нормами и правилами;

2.1.4. запрет на пронос любой электронной и фото-видеоаппаратуры в помещения, используемые для хранения АПД.

2.1.5. Недопустимость перевода документов АПД в электронный формат, за исключением случаев использования в составе ИСПД в соответствии с настоящим положением.

2.1.6. Возложение на работников Учреждения обязанности по соблюдению настоящего положения, Правил и иных нормативных актов Российской Федерации при обработке ПД в составе АПД, привлечение их к дисциплинарной ответственности за нарушение данной обязанности.

2.2. Меры, перечисленные в п.п. 2.1 настоящей главы, реализуются безусловно, непрерывно и в отношении всех имеющихся в распоряжении Учреждения АПД.

2.3. Ответственность за реализацию мер, предусмотренных п. 2.1 настоящей главы, в отношении каждого конкретного АПД возлагается на лицо, ответственное за работу с ним (назначается приказами директора Учреждения) и указанное в этом качестве в Реестре.

3. Действия в случае обнаружения нарушения правил использования АПД

3.1. Лицо, обнаружившее факт нарушения правил использования АПД (несанкционированный доступ, несоблюдение мер, перечисленных в п.п. 2.1. настоящей главы и т.п.), обязано сообщить об этом своему непосредственному руководителю и Уполномоченному лицу.

3.2. По факту обращения, указанного в п.п. 3.1. настоящей главы, Уполномоченное лицо инициирует проверку, для проведения которой могут привлекаться любые необходимые специалисты Учреждения.

3.3. Проверка должна быть проведена и закончена в течение 10 рабочих дней с момента обнаружения факта нарушения правил пользования АПД.

3.4. Срок, предусмотренный п.п. 3.3. настоящей главы, может быть продлен Уполномоченным лицом, но не более чем на 20 рабочих дней.

3.5. Результаты проверки должны быть оформлены в виде заключения, содержащего:
3.5.1. описание выявленных фактов нарушения правил пользования АПД;
3.5.2. выводы о причинах и условиях, приведших к допущенным нарушениям;
3.5.3. предложения о дальнейших действиях, связанных с выявленными нарушениями (инициирование юридических процедур, направленных на привлечение виновных лиц к ответственности и взыскании с них сумм причиненного ущерба, принятие мер по минимизации негативных последствий нарушения для субъектов персональных данных и Учреждения и т.п.);
3.5.4. предложения по устранению причин и условий, приведших к допущенным нарушениям (совершенствование АПД, изменение режима доступа к нему и т.п.).
3.6. Результаты проверки должны быть доведены до сведения лица, ответственного за работу с АПД не позднее одного рабочего дня с момента их оформления. Доведение результатов проверки до сведения лица, обнаружившего факт нарушения правил пользования АПД, осуществляется исключительно по требованию такого лица и при условии, что при этом не разглашаются конфиденциальные сведения, доступ к которым у такого лица отсутствует.

IV. Ответственность

1. Персональная ответственность

1.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
1.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
1.3. Руководитель, разрешающий сотруднику доступ к конфиденциальному документу, несет персональную ответственность за данное разрешение.
1.4. **Лица со специальными полномочиями** несут ответственность:
1.4.1. за рассмотрение и принятие решений (совместно с Уполномоченным лицом) относительно:
- новых точек сбора ПД;
- новых ИС, в которые требуется передать ПД из существующих ИСПД;
- сбора новых ПД в существующие ИСПД.

1.4.2. в системе разрешения доступа к обработке ПД за:
- организацию защиты ПД в Учреждении.
- принятие решений о доступе к обработке ПД (только по ИСПД Учреждения, в которые осуществляется ввод конфиденциальных ПД);
- организацию учета лиц, получивших доступ к обработке ПД в ИСПД;
- организацию сверки по ролям в ИСПД.

1.5. **Уполномоченное лицо** несет ответственность за ведение Реестра ИСПД;
1.6. **Ответственность участников процедуры ответов на запросы** субъектов ПД:
1.6.1. Уполномоченное лицо:
- первичная экспертиза запросов;
- учет и хранение поступивших запросов и ответов на них;
- контроль сроков исполнения процедуры ответов на запросы субъектов ПД участниками процедуры;
- проведение расследований по фактам нарушений режима защиты ПД.

1.6.2. Кадровая (медицинская) служба:
- своевременное исполнение процедуры формирования ответов на запросы субъектов ПД в части ее касающейся;
- учет и хранение запросов и ответов на запросы, обработанных кадровой (медицинской) службой.

1.6.3. Ответственные за работу с ИСПД/АПД:
- достоверность и точность предоставляемой информации по запрашиваемому субъекту ПД;
- проверка факта недостоверности ПД в установленные настоящим Положением сроки;
- блокирование (разблокирование), уничтожение ПД субъекта ПД по решению уполномоченного сотрудника (юриста) в установленные настоящим Положением сроки;
- учет лиц, получивших доступ к обработке ПД в ИСПД;
- ежегодная сверка по ролям и пользователям, обрабатывающим ПД.

1.7. Каждый сотрудник Учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

2. Виды ответственности

2.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД субъектов, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

2.2. **Дисциплинарная ответственность:**

2.2.1. В соответствии со статьей 90 Трудового кодекса РФ сотрудники, нарушившие нормы, регулирующие обработку и защиту персональных данных привлекаются к дисциплинарной ответственности в соответствии со статьей 192 ТК РФ, включая замечание, выговор и увольнение по соответствующему основанию (разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, п.п В. п. 6 ч.1 ст. 81 ТК РФ).

2.3. **Материальная ответственность:**

2.3.1. Согласно статьям 238, 242 ТК РФ все сотрудники несут персональную (в т.ч. материальную) ответственность за ущерб, причиненный работодателю. Работник несет материальную ответственность как за прямой действенный ущерб, причиненный им работодателю, так и за ущерб, возникший у работодателя в результате возмещения им ущерба, причиненного работником третьим лицам.

2.3.2. За причиненный ущерб работник несет материальную ответственность в пределах своего среднего месячного заработка, если иное не предусмотрено настоящим Кодексом или иными федеральными законами (статья 241 ТК РФ).

2.3.3. Согласно п. 7 статьи 243 ТК РФ за разглашение сведений, составляющих охраняемую законом тайну (государственную, служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, работники несут материальную ответственность в полном размере причиненного ущерба

2.4. **Административная ответственность:**

2.4.1. Согласно статье 13.11. Кодекса Российской Федерации об административных правонарушениях (от 30 декабря 2001 г. № 195-ФЗ) нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц - от пятисот до одной тысячи рублей; на юридических лиц - от пяти тысяч до десяти тысяч рублей.

2.4.2. Статья 13.14. гласит - Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей; на должностных лиц - от четырех тысяч до пяти тысяч рублей.

2.5. **Уголовная ответственность** наступает в соответствии со статьей 137 Уголовного кодекса РФ за нарушение неприкосновенности частной жизни:

2.5.1. Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации - наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок до одного года, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

2.5.2. Те же деяния, совершенные лицом с использованием своего служебного положения, - наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо арестом на срок от четырех до шести месяцев, либо лишением свободы на срок от одного года до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

2.6. Если права и законные интересы субъекта ПД были нарушены в связи с разглашением информации, содержащей его ПД, или иным неправомерным использованием такой информации, он вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с иском о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации.

Перечень приложений

к **Положению о порядке обработки и защиты персональных данных в Негосударственном учреждении «Медицинский центр «Родник»**

Приложение № 1	Форма Журнала учета сведений о поступающем запросе
Приложение № 2	Форма Согласия на обработку персональных данных (для работников)
Приложение № 3	Форма Согласия на обработку персональных данных (для пациентов)
Приложение № 4	Перечень должностей, допущенных к работе с персональными данными
Приложение № 5	Форма Допуска к персональным данным
Приложение № 6	Перечень персональных данных обрабатываемых Учреждением (работников, контрагентов, кандидатов, несписочного состава, пациентов)
Приложение № 7	Форма Обязательства по обеспечению конфиденциальности персональных данных (для работников)
Приложение № 8	Форма обязательства по обеспечению конфиденциальности персональных данных (для физических лиц)
Приложение № 9	Форма Расписки в ознакомлении с Перечнем обрабатываемых персональных данных