МУНИЦИПАЛЬНОЕ МЕДИЦИНСКОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ

«ГОРОДСКАЯ ПОЛИКЛИНИКА № 5»

ПРИКАЗ

№ 383 27 марта 2017 г.

Об утверждении политики оператора в отношении обработки персональных данных и политики безопасности персональных данных

В целях выполнения требований Конституции РФ, Трудового кодекса РФ № 197-ФЗ от 30.12.2001 г., Федерального закона РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 г., Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Указа Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997 г. и других нормативных и правовых актов, регулирующих процессы обработки персональных данных (далее – ПДн).

ПРИКАЗЫВАЮ:

1. Утвердить политику оператора в отношении обработки персональных данных (Приложение 1);
2. Утвердить политику безопасности персональных данных (Приложение 2);
3. Никитиной Е.А., начальнику организационно- методического отдела ознакомить всех сотрудников, задействованных в обработке персональных с политикой оператора в отношении обработки персональных данных и политикой безопасности персональных данных в ММАУ «Городская поликлиника № 5»;

Контроль исполнения приказа оставляю за собой.

Главный врач Беленькая В.А.

Приложение 1
к приказу ММАУ «Городская поликлиника № 5»
№ 383 от 27 марта 2017 г.

ПОЛИТИКА
оператора в отношении обработки персональных данных

1. Общие положения

1. В целях гарантирования выполнения норм федерального законодательства в полном объеме ММАУ «Городская поликлиника No5» (далее - Оператор) считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных (далее - ПДн), а также обеспечение безопасности процессов их обработки.
2. Настоящая Политика оператора в отношении обработки ПДн в ММАУ «Городская поликлиника № 5» (далее - Политика) характеризуется следующими признаками:
- Разработана в целях обеспечения реализации требований законодательства Российской Федерации в области обработки ПДн субъектов ПДн.
- Раскрывает основные категории ПДн, обрабатываемых Оператором, цели, способы и принципы обработки Оператором ПДн, права и обязанности Оператора при обработке ПДн, права субъектов ПДн, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности ПДн при их обработке.
- Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке ПДн.

2. Информация об Операторе

Наименование: Муниципальное медицинское автономное учреждение «Городская Поликлиника № 5».
ИНН: 7204036223.
Фактический адрес: 625049, г. Тюмень, ул. Московский тракт. 35 А
Тел., факс 8(3452) 56-02-31.
Филиалы: 625062, г. Тюмень, ул. Николая Чаплина 115/9,
625025, г. Тюмень, ул. Волгоградская, 117/2
625032, г. Тюмень, ул. Червишевский тракт, 68а/1
625007, г. Тюмень, ул. Николая Чаплина, 117/1 а
625062, г. Тюмень, ул. Федюнинского, 5а
625007, г. Тюмень, ул. Депутатская, 127
625000, Тюменский район, д. Патрушева, ул. Ветеранов, д. 16а

3. Основные понятия

Для целей настоящей Политики используются следующие понятия:
1. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.
2. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).
3. Субъект - субъект ПДн.
4. Работник - физическое лицо, состоящее в трудовых отношениях с оператором.
5. Обработка ПДн - любое действие (операция) или совокупность действий

(операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.
6. Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.
7. Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.
8. Предоставление ПДн - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.
9. Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).
10. Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в информационной системе персональных данных (далее - ИСПДн) и (или) в результате которых уничтожаются материальные носители ПДн.
11. Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.
12. Информационная система персональных данных - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.
13. Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

4. Правовые основания обработки ПДн

1. Политика Оператора в области обработки ПДн, а также основание для обработки ПДн определяются в соответствии со следующими нормативными правовыми актами Российской Федерации:
- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Федеральным законом от 19.12.2005 No 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- Федеральным законом от 27.07.2006 No 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 No 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом от 29.11.2010 N 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации».

5. Цели обработки ПДн

1. Оператор обрабатывает ПДн исключительно в следующих целях:
   - Исполнения положений нормативных актов, указанных в пункте 4, подпункт 1.
   - Принятия решения о трудоустройстве кандидата в учреждение ММАУ «Городская поликлиника № 5».
   - Заключения и выполнения обязательств по трудовым договорам, договорам гражданско-правового характера и договорам с контрагентами;
   - Предоставление медицинской помощи.

6. Категории обрабатываемых ПДн, источники их получения, сроки обработки и хранения

1. В ИСПДн Оператора обрабатываются следующие категории ПДн:
   - Сотрудников Оператора (Административно-управленческий состав, врачи, обслуживающий персонал);
   - Уволенных сотрудников ММАУ «Городская поликлиника No5»;
   - Физических лиц, обращающихся для зачисления в кадровый резерв ММАУ «Городская поликлиника No5»;
   - Физических лиц получающих медицинскую помощь в учреждении ММАУ «Городская поликлиника No5».
2. Сроки обработки и хранения ПДн определены в «Перечне обрабатываемых ПДн.

7. Основные принципы обработки, передачи и хранения ПДн

1. Оператор в своей деятельности обеспечивает соблюдение принципов обработки ПДн, указанных в ст. 5 Федерального закона от 27.07.2006 No 152-ФЗ «О персональных данных».
2. Оператор не осуществляет обработку биометрических ПДн (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность).
3. Оператор выполняет обработку специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.
4. Оператор не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу ПДн.
5. Все электронные базы данных содержащие ПДн являющихся гражданами РФ и технические средства с помощью которых осуществляется обработка ПДн субъектов, являющихся гражданами РФ находятся на территории РФ;
6. Оператором созданы общедоступные источники ПДн (справочники, адресные книги). ПДн, сообщаемые субъектом (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и др.), включаются в такие источники только с письменного согласия субъекта ПДн.

8. Сведения о третьих лицах, участвующих в обработке ПДн

1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов ПДн, Оператор, в ходе своей деятельности предоставляет ПДн следующим организациям:
- Федеральной налоговой службе;
- Пенсионному фонду России (только о субъектах, являющихся сотрудниками Оператора);
- Страховым компаниям (только о субъектах, являющихся сотрудниками Оператора);
- Кредитным организациям;
- федеральному и территориальному фондам обязательного медицинского страхования;
- организациям (учреждениям), осуществляющим на законном основании обработку медико-статистической информации;
- органам управления здравоохранением по Тюменской области (без автономных округов), муниципальных образований, расположенных на территории Тюменской области (без автономных округов).
2. Оператор не поручает обработку ПДн другим лицам на основании договора.

9. Меры по обеспечению безопасности ПДн при их обработке

1. Оператор при обработке ПДн принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.
Обеспечение безопасности ПДн достигается, в частности, следующими способами:
- Назначением ответственных за организацию обработки ПДн;
- Осуществлением внутреннего контроля и аудита соответствия обработки ПДн Федеральному закону от 27.07.2006 No 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам;
- Ознакомлением работников Оператора, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами в отношении обработки ПДн, и обучением указанных сотрудников;
- Определением угроз безопасности ПДн при их обработке в ИСПДн;
- Применением организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
- Оценкой эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;
- Учетом машинных носителей ПДн;
- Выявлением фактов несанкционированного доступа к ПДн и принятием соответствующих мер;
- Восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- Установлением правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- Контролем за принимаемыми мерами по обеспечению безопасности ПДн и уровнем защищенности ИСПДн.

2. Обязанности должностных лиц, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются приказами главного врача.

10. Обработка ПДн

1. Общие требования при обработке ПДн.
В целях обеспечения прав и свобод человека и гражданина при обработке ПДн соблюдаются следующие требования:

1.2. Обработка ПДн допускается в следующих случаях:
- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;
- обработка ПДн необходима для осуществления прав и законных интересов оператора или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн

невозможно;

- обработка ПДн осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания ПДн за исключением целей, указанных в Федеральном законе от 27.07.2006 No 152-ФЗ «О персональных данных»;
- осуществляется обработка ПДн, доступ неограниченного круга лиц, к которым предоставлен субъектом ПДн либо по его просьбе (далее - ПДн, сделанные общедоступными субъектом ПДн);
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

1.3. Обработка ПДн должна осуществляться на законной и справедливой основе.

1.4. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.

1.5. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

1.6. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

1.7. При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

1.8. Субъекты ПДн не должны отказываться от своих прав на сохранение и защиту ПДн.

1.9. Порядок рассмотрения запросов субъектов ПДн или их представителей осуществляется в соответствии с «Инструкцией по обработке запросов субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных», утвержденной Оператором.

2. Получение ПДн:

2.1. Все ПДн следует получать непосредственно от субъекта ПДн. Субъект самостоятельно принимает решение о предоставлении своих ПДн, и дает письменное согласие на их обработку оператором. Типовая форма заявления-согласия субъекта на обработку ПДн представлена в приложении 1 к настоящей Политике.

2.2. Если предоставление ПДн является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн, согласно приложению 7 к настоящей Политике.

2.3. В случае недееспособности либо несовершеннолетия субъекта ПДн все ПДн субъекта следует получать от его законных представителей. Законный представитель самостоятельно принимает решение о предоставлении ПДн своего подопечного и дает письменное согласие на их обработку оператором. Типовая форма заявления-согласия на обработку ПДн подопечного представлена в приложении 4 к настоящей Политике.

2.4. Письменное согласие не требуется, если обработка ПДн осуществляется в случаях, указанных в пункте 10 подпункт 1 настоящей Политике.

2.5. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае недееспособности либо несовершеннолетия субъекта ПДн согласие может быть отозвано законным представителем субъекта ПДн. Типовая форма отзыва согласия на обработку ПДн представлена в приложении 3 к настоящей Политике.

2.6. В случаях, когда оператор может получить необходимые ПДн субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее. В уведомлении оператор обязан указать:
- наименование и адрес оператора;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- права субъекта ПДн;
- источник получения ПДн.

Типовая форма уведомления субъекта о получении его ПДн от третьей стороны представлена в приложении 5 к настоящей Политике.

2.7. Запрещается получать и обрабатывать ПДн субъекта о его политических, религиозных и иных убеждениях и частной жизни.

2.8. Запрещается получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.9. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

3. Хранение ПДн:

3.1. Хранение ПДн субъектов осуществляется структурными подразделениями оператора в соответствии с перечнями ПДн и ИСПДн, утвержденными у Оператора.

3.2. Личные дела сотрудников хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа (или металлических шкафах), обеспечивающего защиту от несанкционированного доступа.

3.3. Подразделения, хранящие ПДн на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно постановлению Правительства Российской Федерации от 15.09.2008 No 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования
средств автоматизации».

4. Передача ПДн:

4.1. При передаче ПДн субъекта оператор обязан соблюдать следующие требования:
- не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами. Форма заявления-согласия субъекта на передачу его ПДн третьей стороне см. в приложении 6 настоящей Политики;
- предупредить лиц, получающих ПДн 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 ПДн субъекта, обязаны соблюдать требования конфиденциальности;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции;
- передавать ПДн субъекта представителям субъектов в порядке,

установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми ПДн субъекта, которые необходимы для выполнения указанными представителями их функций;
- все сведения о передаче ПДн субъекта регистрируются в Журнале учета передачи ПДн в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи ПДн или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

4.2. Все меры конфиденциальности при сборе, обработке и хранении ПДн субъекта распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

4.3. Доступ работников к ПДн разрешен в соответствии со списками, утвержденными приказом от 20.08.2015 No «Об организации работ по обеспечению безопасности персональных данных при их обработке, в том числе в информационных системах персональных данных».

4.4. Все сотрудники, имеющие доступ к ПДн субъектов, обязаны подписать обязательство о неразглашении ПДн.

4.5. Передача ПДн осуществляется в организации, указанные в пункте 8 настоящей Политики.

5. Уничтожение ПДн:

5.1. ПДн субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5.2. Документы, содержащие ПДн, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

11. Права и обязанности субъектов ПДн и оператора

1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:
- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом от 27.07.2006 No 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные действующим законодательством Российской Федерации.

2. В целях обеспечения защиты ПДн, субъекты имеют право:
- требовать от оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими,

неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать предоставления сведений, указанных в пункте 11 подпункте 1 от оператора в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн;
- требовать предоставления сведений, указанных в пункте 11 подпункте 1, от оператора при обращении либо при получении запроса субъекта ПДн или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации;
- требовать исключения или исправления неверных или неполных ПДн, а также данных, обработанных с нарушением законодательства;
- при отказе оператора или уполномоченного им лица исключить или исправить ПДн субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;
- дополнить ПДн оценочного характера заявлением, выражающим его собственную точку зрения;
- требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите ПДн субъекта.
- Субъект ПДн или его законный представитель обязуется предоставлять ПДн, соответствующие действительности.

12. Ответственность за нарушение норм, регулирующих обработку и защиту ПДн

1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему ПДн, несет персональную ответственность за данное разрешение.
2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

13. Контактная информация

Ответственным за организацию обработки ПДн в учреждении ММАУ «Городская поликлиника No5», назначен начальник организационно- методического отдела Никитина Елена Афанасьевна
тел.: 8(3452) 56-02-31;
E-mail: gp5@med-to.ru
Уполномоченным органом по защите прав субъектов ПДн является Федеральная

служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
(Роскомнадзор), Управление по защите прав субъектов ПДн.
Управление Роскомнадзора по Тюменской области, Ханты-Мансийскому автономному округу - Югре и Ямало-Ненецкому автономному округу:
Адрес: ул. Республики, д. 12, г. Тюмень, 625003.
Тел.: (3452) 46-17-61.
Факс: (3452) 46-60-46. E-mail: rsoc72@rsoc.ru. Сайт: 72.rsoc.ru

Приложение 2

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

СОГЛАСИЕ
субъекта персональных данных, обратившегося в медицинскую организацию, на обработку его персональных данных

Я,
_____,
(Ф.И.О. полностью)
паспорт _____, выдан_____
(серия и номер)
_____,
(дата и наименование выдавшего органа)
проживающий по адресу:
_____
(по месту регистрации)
в соответствии с требованиями Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных», подтверждаю свое согласие на обработку
ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а (далее – Оператор) моих персональных данных, включающих: фамилию, имя, отчество, год, месяц, дату и место рождения, пол, гражданство, место жительства, в том числе сведения о регистрации по месту жительства, месту проживания, место работы, социальное положение (статус), реквизиты документа, удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа выдавшего документ), реквизиты полисов медицинского страхования, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), сведения об оказанной медицинской помощи, сведения о мерах социальной поддержки, данные о состоянии здоровья, в том числе, содержащие врачебную тайну в целях:
– установления медицинского диагноза, оказания медицинских и медико- социальных услуг, в медико- профилактических целях при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством
Российской Федерации сохранять врачебную тайну;
– защиты моих прав на получение качественной медицинской помощи;

– осуществления контроля качества оказанных мне медицинских услуг, проведения медико- профилактических мероприятий;
–оплаты оказанных по программе обязательного и добровольного медицинского страхования медицинских услуг;
– ведения учета оказанной медицинской помощи;
– формирования медицинских статистических данных в формах медико- статистического наблюдения;
– обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов Российской Федерации.
Предоставляю Оператору право осуществлять при обработке моих персональных данных все действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Оператор вправе обрабатывать мои персональные данные посредством внесения их в информационные хранилища (электронную базу данных, списки, реестры, регистры), а также учетные и отчетные формы в электронном и бумажном исполнении.
Оператор вправе осуществлять обработку моих персональных данных централизованно в Единой государственной информационной системе в сфере здравоохранения, отраслевой информационной системе здравоохранения Тюменской области.
Оператор имеет право получать и передавать мои персональные данные, в том числе содержащие сведения, составляющие врачебную тайну, с использованием средств автоматизации и без использования таких средств, на материальных носителях, в том числе в бумажном виде в следующие государственные органы, организации (учреждения):
– федеральному и территориальному фондам обязательного медицинского страхования;
– пенсионному фонду Российской Федерации, включая его территориальные органы;
– страховым медицинским организациям, осуществляющим мое страхование;
– организациям (учреждениям), осуществляющим на законном основании обработку медико- статистической информации;
– органам управления здравоохранением Тюменской области (без автономных округов), муниципальных образований, расположенных на территории Тюменской области (без автономных округов);
– иным медицинским организациям Российской Федерации (регионального и федерального уровней) на законном основании осуществляющих свою медицинскую деятельность, для установления мне медицинского диагноза, определения тактики лечения, оказание медицинских и медико- социальных услуг, в медико- профилактических целях при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять медицинскую тайну.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Подпись субъекта персональных данных_____

Для контроля качества оказываемых мне медицинских услуг, я подтверждаю свое согласие на сбор речевой информации при оказании мне медицинских услуг в данной медицинской организации. Настоящим я подтверждаю, что данные речевой информации могут быть предоставлены Департаменту здравоохранения Тюменской области с целью контроля соблюдения этики и качества оказываемых мне медицинских услуг.

В случае несогласия на сбор речевой информации, пациенту необходимо собственноручно вписать отказ и утвердить его личной подписью.

Незаполненная графа «Подпись субъекта персональных данных» толкуется, как согласие пациента на сбор речевой информации.

Подпись субъекта персональных данных_____

Настоящее согласие дано мной «_____»_____и действует бессрочно, в случае если согласие не отозвано в письменной форме.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного заявления, который может быть направлен в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи и предоставления соответствующей медико-статистической информации.

Приложение 3

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

СОГЛАСИЕ
работника медицинской организации на обработку его персональных данных

Я,

_____,

(Ф.И.О. полностью)

паспорт _____, выдан_____

(серия и номер)

_____,

(дата и наименование выдавшего органа)

проживающий по адресу:

_____

(по месту регистрации)

в соответствии с требованиями Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных» и с целью обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обеспечения моей личной безопасности, контроля Работодателем за количеством и качеством выполняемой работы, сохранности личного имущества и имущества Работодателя, даю согласие ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а), на любые действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ)*, обезличивание, блокирование, удаление, уничтожение нижеследующих персональных данных: фамилия, имя, отчество; год месяц, дата рождения; место рождения; пол; гражданство, место жительства, в том числе сведения о регистрации по месту жительства, месту проживания; социальное положение (статус), реквизиты документа, удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа выдавшего документ), изображение лица (в электронном или бумажном виде) состояние в браке, состав семьи; место работы, профессия (специальность); общий трудовой стаж, сведения о приемах, перемещениях и увольнениях по предыдущим местам работы; сведения, включенные в трудовую книжку; образование и повышение квалификации или наличие специальных знаний; сведения о воинском учете; идентификационный номер налогоплательщика; номер страхового свидетельства государственного пенсионного страхования; номер полиса обязательного медицинского страхования; сведения о доходах; информация по лицевому банковскому счету работника; иные персональные данные, учитываемые в формах статистического и медико- статистического наблюдения и информационных системах органов управления здравоохранением федерального и территориального уровней;

Оператор вправе, при получении письменного согласия членов семьи, производить обработку персональных данных членов семьи, родственников.

Оператор вправе обрабатывать мои персональные данные посредством внесения их в информационные хранилища (электронную базу данных, списки, реестры, регистры), а также учетные и отчетные формы в электронном и бумажном исполнении.

Оператор вправе осуществлять обработку моих персональных данных централизованно в Единой государственной информационной системе в сфере

здравоохранения, отраслевой информационной системе здравоохранения Тюменской области.

*Оператор вправе передавать мои персональные данные в налоговые органы; правоохранительные органы (при официальном запросе); военкоматы; органы социального страхования, государственные внебюджетные фонды; банки (для оформления пластиковой карты) без дополнительного письменного согласия, в объеме и случаях предусмотренных действующим законодательством РФ; организациям (учреждениям), осуществляющим на законном основании обработку медико-статистической информации; органам управления здравоохранением Тюменской области (без автономных округов), муниципальных образований, расположенных на территории Тюменской области (без автономных округов).

Настоящее согласие вступает в силу со дня его подписания.

Настоящее согласие действует до получения оператором в письменной форме отзыва согласия на обработку.

Подтверждаю, что права и обязанности в области защиты персональных данных мне разъяснены, а также право работодателя обрабатывать (в том числе и передавать) часть моих персональных данных без моего согласия, в соответствии с законодательством Российской Федерации.

Подтверждаю, что отзыв согласия производится в письменном виде в соответствии с действующим законодательством. Всю ответственность за неблагоприятные последствия отзыва согласия беру на себя.

Подпись субъекта персональных данных_____

Приложение 4

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

_____

(наименование оператора)

_____

(адрес оператора)

_____

(Ф.И.О. субъекта персональных данных)

_____

(адрес регистрации субъекта персональных данных)

_____

(наименование, серия, номер

основного документа, удостоверяющего личность)

_____

(дата выдачи указанного документа)

_____

(наименование органа выдавшего документ)

Типовая форма

отзыва согласия на обработку персональных данных

Прошу прекратить обработку моих персональных данных в связи с_____

_____

_____

(указать причину)

_____20 г. _____

(подпись)

Приложение 5

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

СОГЛАСИЕ
законного представителя субъекта персональных данных на обработку персональных данных субъекта персональных данных обратившегося в медицинскую организацию

Я, _____,
(Ф.И.О. полностью)
паспорт _____, выдан _____
(серия и номер)
_____,
(дата и наименование выдавшего органа)
проживающий по адресу: _____,
(по месту регистрации)
являющийся законным представителем
_____
(родителем, усыновителем, опекуном, попечителем)
представляемого _____
(фамилия, имя, отчество сына (дочери), усыновленного (удочеренной), подопечного (подопечной)
дата рождения «___» _____ ____ г., _____
_____
(реквизиты документа, удостоверяющего личность (при наличии)
проживающего по адресу: _____,
(по месту регистрации)
_____
(реквизиты документа, подтверждающего полномочия представителя)
в соответствии с требованиями Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных», подтверждаю свое согласие на обработку ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а (далее – Оператор) моих персональных данных, включающих: фамилию, имя, отчество, год, месяц, дату и место рождения, пол, гражданство, место жительства, в том числе сведения о регистрации по месту жительства, месту проживания, место работы, социальное положение (статус), реквизиты документа, удостоверяющего личность (серия, номер, дата выдачи, наименование и код подразделения органа выдавшего документ), реквизиты полисов медицинского страхования, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), сведения об оказанной медицинской помощи, сведения о мерах социальной поддержки, данные о состоянии здоровья, в том числе, содержащие врачебную тайну в целях:

– установления медицинского диагноза, оказания медицинских и медико- социальных услуг, в медико- профилактических целях при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

– защиты моих прав на получение качественной медицинской помощи;

– осуществления контроля качества оказанных мне медицинских услуг, проведения медико- профилактических мероприятий;

–оплаты оказанных по программе обязательного и добровольного медицинского страхования медицинских услуг;

– ведения учета оказанной медицинской помощи;
– формирования медицинских статистических данных в формах медико- статистического наблюдения;
– обеспечения соблюдения законов Российской Федерации и иных нормативных правовых актов Российской Федерации.
Предоставляю Оператору право осуществлять при обработке моих персональных данных все действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Оператор вправе обрабатывать мои персональные данные посредством внесения их в информационные хранилища (электронную базу данных, списки, реестры, регистры), а также учетные и отчетные формы в электронном и бумажном исполнении.
Оператор вправе осуществлять обработку моих персональных данных централизованно в Единой государственной информационной системе в сфере здравоохранения, отраслевой информационной системе здравоохранения Тюменской области.
Оператор имеет право получать и передавать мои персональные данные, в том числе содержащие сведения, составляющие врачебную тайну, с использованием средств автоматизации и без использования таких средств, на материальных носителях, в том числе в бумажном виде в следующие государственные органы, организации (учреждения):
– федеральному и территориальному фондам обязательного медицинского страхования;
– пенсионному фонду Российской Федерации, включая его территориальные органы;
– страховым медицинским организациям, осуществляющим мое страхование;
– организациям (учреждениям), осуществляющим на законном основании обработку медико- статистической информации;
– органам управления здравоохранением Тюменской области (без автономных округов), муниципальных образований, расположенных на территории Тюменской области (без автономных округов);
– иным медицинским организациям Российской Федерации (регионального и федерального уровней) на законном основании осуществляющих свою медицинскую деятельность, для установления мне медицинского диагноза, определения тактики лечения, оказание медицинских и медико- социальных услуг, в медико- профилактических целях при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять медицинскую тайну.
Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Подпись законного представителя (родителя, усыновителя, опекуна, попечителя)_____

Для контроля качества оказываемых мне медицинских услуг, я подтверждаю свое согласие на сбор речевой информации при оказании мне медицинских услуг в данной медицинской организации. Настоящим я подтверждаю, что данные речевой информации могут быть предоставлены Департаменту здравоохранения Тюменской области с целью контроля соблюдения этики и качества оказываемых мне медицинских услуг.

В случае несогласия на сбор речевой информации, пациенту необходимо собственноручно вписать отказ и утвердить его личной подписью.

Незаполненная графа «Подпись субъекта персональных данных» толкуется, как согласие пациента на сбор речевой информации.

Подпись законного представителя (родителя, усыновителя, опекуна, попечителя)_____

Настоящее согласие дано мной «_____»_____и действует бессрочно, в случае если согласие не отозвано в письменной форме.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного заявления, который может быть направлен в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи и предоставления соответствующей медико-статистической информации.

Приложение 6

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

Типовая форма
уведомления субъекта о начале обработки его персональных данных, полученных у третьей стороны.

_____,
(фамилия, имя, отчество)
_____,
(адрес субъекта персональных данных)
ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а, уведомляет Вас о начале обработки Ваших персональных данных с целью
_____
(цель обработки персональных данных)
на основании положений _____
Персональные данные, а именно _____,
получены от_____.
К Вашим персональным данным имеют доступ следующие категории сотрудников
_____.
Согласно Федеральному закону от 27.07.2006 № 152- ФЗ «О персональных данных»
Вы имеете право:
– на получение сведений о ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а (далее - Оператор), как операторе персональных данных, месте его нахождения, о наличии оператора Ваших персональных данных;
– на ознакомление с Вашими персональными данными, если это не влечет за собой нарушения конституционных права и свободы других лиц;
– требовать отоператора уточнения Ваших персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите Ваших прав;
– получать при обращении информацию, касающуюся обработки Ваших персональных данных, в том числе содержащую:
подтверждение факта обработки, а также цель такой обработки;
способы обработки, применяемые оператором;
сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
перечень обрабатываемых персональных данных и источник их получения;
сроки обработки Ваших персональных данных, в том числе сроки их хранения.
– в случаях возникновения оснований считать, что оператор осуществляет обработку Ваших персональных данных с нарушением требований Федерального закона или иным образом нарушает Ваши права и свободы, обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
– на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке
_____20 г. _____(подпись)

Приложение 7

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

Типовая форма
заявления – согласия субъекта на передачу его персональных данных третьей стороне

Я, _____,
проживающий (- ая) по адресу: _____ ,
паспорт серии _____, номер _____,
выданный
_____
« ___ » _____ года,
в соответствии со ст. 12 Федерального закона от 27.07.2006 № 152 – ФЗ «О персональных данных», даю согласие на передачу моих персональных данных
ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а,
а именно:

_____
_____
_____

(указать состав персональных данных (Ф.И.О, паспортные данные, адрес ...)

Обработка вышеуказанных персональных данных будет осуществляться путем:

_____
_____

(Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных)

для обработки в целях:

_____
_____
_____

следующим лицам:

_____
_____
_____

(указать Ф.И.О. физического лица или наименование организации и адрес, которым сообщаются данные)

Я также утверждаю, что ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а также с моими правами и обязанностями в этой области.
Согласие вступает в силу со дня его подписания и действует в течение _____ .
Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

_____20_____г. _____

(подпись)

Приложение 8

к приказу ММАУ «Городская поликлиника № 5»

от _____ № _____

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные.

Разъяснения
юридических последствий отказа предоставить свои персональные данные, субъектом в связи с поступлением на работу или выполнением работы

Мне,_____
разъяснены юридические последствия отказа предоставить свои персональные данные ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а.

В соответствии со статьями 57, 65, 69 Трудового кодекса Российской Федерации субъект персональных данных, поступающих на работу или работающий, обязан представить определенный перечень информации о себе.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

На основании пункта 11 части 1 статьи 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

_____20__ г. _____
(подпись)

Разъяснения
юридических последствий отказа предоставить свои персональные данные, субъектом в связи с оказанием услуг

Мне,_____
разъяснены юридические последствия отказа предоставить свои персональные данные ММАУ «Городская поликлиника № 5», расположенного по адресу: 625049, Российская Федерация, Тюменская область, г. Тюмень, ул. Московский тракт, 35а.

В соответствии с Гражданским кодексом Российской Федерации субъект персональных данных обязан представить определенный перечень информации о себе.

Без представления субъектом персональных данных обязательных для заключения договора сведений, договор не может быть заключен.

_____20__ г. _____
(подпись

Приложение II
к приказу ММАУ «Городская поликлиника № 5»
№ 383 от 27 марта 2017 г.

П О Л И Т И К А

безопасности персональных данных

ММАУ «Городская поликлиника 5»

г. Тюмень – 2017

Оглавление

Список терминов и определений

Организация – ММАУ «Городская поликлиника №5»

ПДн – персональные данные.

ИСПДн – информационная система персональных данных.

АРМ – автоматизированное рабочее место.

СЗПДн – система защиты персональных данных.

1. Общие положения

Настоящий документ устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Политика разработана в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет порядок защиты персональных данных, обрабатываемых в Организации.

1.1. Цель политики.

Определить требования безопасности к персональным данным, обрабатываемым в информационных системах персональных данных Организации, с целью предотвращения любого несанкционированного доступа.

Критичным фактором безопасности ПДн является организация эффективного контроля доступа к ПДн, обрабатываемых в информационных системах персональных данных. Отсутствие адекватного контроля доступа может вести к несанкционированному доступу к ИСПДн Организации.

1.2. Область применения.

Требования настоящей Политики распространяются на всех сотрудников Организации (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

2. Состав и содержание мер по обеспечению безопасности ПДн и план работ по защите ПДн, обрабатываемых в ИСПДн Организации

2.1. Состав и содержание мер по обеспечению безопасности ПДн

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).
- Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.
- Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.
- Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.
- Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.
- Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
- Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

- Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.
- Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.
- Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.
- Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.
- Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.
- Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.
- Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.
- Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Для реализации указанных мер по обеспечению безопасности могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации.

Для защиты ПДн, представленной в виде информативных электрических сигналов и физических полей могут применяться следующие методы и способы защиты информации:

- использование технических средств в защищенном исполнении;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- размещение объектов защиты в соответствии с предписанием на эксплуатацию;
- размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
- обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
- обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

Возможные методы и способы защиты ПДн, представленных в виде акустической (речевой) информации, заключаются в реализации организационных и технических мер для обеспечения звукоизоляции ограждающих конструкций помещений, в которых расположена информационная система, их систем вентиляции и кондиционирования, не позволяющей вести прослушивание акустической (речевой) информации при голосовом вводе персональных данных в информационной системе или воспроизведении информации акустическими средствами.

2.2. Принципы и способы определения актуальных угроз безопасности ПДн

Для выбора и реализации мер по обеспечению безопасности ПДн в информационной системе Организации назначается ответственный по защите информации в информационных системах персональных данных.

Выбор и реализация мер по обеспечению безопасности ПДн в ИСПДн осуществляются на основе, определяемых в Организации, угроз безопасности персональных данных (модель угроз) и в зависимости уровня защищенности ПДн, определенного в соответствии с Постановлением Правительства от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Модель угроз разрабатывается на основе следующих методических документов:

- Базовая модель угроз безопасности персональным данным при обработке в информационных системах персональных данных, утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;
- Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России.

Модель угроз персональным данным составляется ответственным по защите ПДн и утверждается руководителем Организации.

Периодичность пересмотра модели угроз для каждой ИСПДн определена в пункте 2.4. данного документа.

2.3. Определение уровня защищенности ПДн

При обработке персональных данных в информационных системах устанавливаются уровни защищенности ПДн в соответствии с Постановлением Правительства от 1.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

При определении уровня защищенности ПДн, при их обработке в ИСПДн учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- тип угроз безопасности ПДн, актуальных для информационной системы;
- проверяется условие принадлежности ПДн сотрудникам оператора ПДн или иным субъектам, не являющимся сотрудниками оператора.

По результатам анализа исходных данных информационных систем персональных данных присваивается соответствующий уровень защищенности ПДн, и составляется «Акт определения уровня защищенности ПДн, при их обработке в ИСПДн», утверждаемый руководителем Организации.

Уровень защищенности персональных данных может быть пересмотрен:

- по решению ответственного по защите ПДн в Организации на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

2.4. План мероприятий по обеспечению безопасности ПДн

Для обеспечения безопасности процессов обработки персональных данных в Организации, должны быть выполнены работы, в соответствии с планом, указанном ниже:

Мероприятие	Периодичность
Организационные мероприятия	
Обследование информационных систем персональных данных	Разовое
Определение перечня ИСПДн	Разовое
Определение обрабатываемых ПДн и объектов защиты	Разовое
Определение круга лиц, участвующих в обработке ПДн	Разовое
Определение ответственности лиц, участвующих в обработке	Разовое
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое
Назначение ответственных за безопасность и организацию ИСПДн	Разовое
Определение уровня защищенности ПДн для всех выявленных ИСПДн	Разовое
Установление контролируемой зоны вокруг ИСПДн	Разовое
Выбор помещений для установки аппаратных средств ИСПДн в помещениях, с целью исключения НСД лиц, не допущенных к обработке ПДн	Разовое
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое
Организация порядка резервного копирования и восстановления защищаемой информации на твердые носители	Разовое
Введение в действие инструкции по защите ИСПДн	Разовое
Организация информирования и обучения сотрудников о порядке обработки и защиты ПДн	Разовое
Разработка должностных инструкций о порядке обработки ПДн и обеспечении введенного режима защиты	Разовое
Разработка инструкций о действии в случае возникновения внештатных ситуаций	Разовое
Разработка положения об обработке и защите ПДн, обрабатываемых в ИСПДн	Разовое
Утверждение политики безопасности персональных данных	Разовое
Организация журнала учета обращений субъектов ПДн	Разовое
Организация перечня по учету технических средств и средств защиты, а также документации к ним	Разовое
Организация постов охраны для пропуска в контролируемую зону	Разовое

Мероприятие	Периодичность
Инженерно-технические мероприятия	
Внедрение технической системы контроля доступа в контролируемую зону и помещения	Разовое
Внедрение технической системы контроля доступа к элементам ИСПДн	Разовое
Установка жалюзи на окнах	Разовое
Внедрение резервных (дублирующих) технических средств ключевых элементов ИСПДн	Разовое
Мероприятия по внедрению СЗИ от НСД	
Внедрение системы защиты от НСД на рабочих станциях и серверах	Разовое
Внедрение системы антивирусной защиты	Разовое
Внедрение средств межсетевого экранирования	Разовое
Внедрение средств анализа защищенности	Разовое
Внедрение средств обнаружения вторжений	Разовое
Создание журнала внутренних проверок и поддержание его в актуальном состоянии	Ежемесячно
Контроль над соблюдением режима обработки ПДн	Еженедельно
Контроль над соблюдением режима защиты	Ежедневно
Контроль над выполнением антивирусной защиты	Еженедельно
Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно
Контроль за обеспечением резервного копирования	Ежемесячно
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	Ежегодно
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно
Контроль за разработкой и внесением изменений в программное обеспечение собственной разработки или штатное ПО, специально дорабатываемое собственными разработчиками или сторонними организациями.	Ежемесячно
Тестирование реализации правил фильтрации на МЭ, настроек системы защиты от НСД, системы защиты от вирусов, системы	Ежемесячно

Мероприятие	Периодичность
обнаружения вторжений и анализа защищенности	

3. Требования по обеспечению безопасности персональных данных

Выбранные и реализованные меры по обеспечению безопасности ПДн должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных, при их обработке в информационных системах в составе системы защиты персональных данных Организации.

Система защиты персональных данных, строится на основании:

- Модели угроз безопасности персональным данным при их обработке в информационной системе персональных данных «Сотрудники» ММАУ «Городская поликлиника №5»;
- Модели угроз безопасности персональным данным при их обработке в информационной системе персональных данных «Пациенты» ММАУ «Городская поликлиника №5»;
- Технического проекта «системы защиты персональных данных информационных систем персональных данных ММАУ «Городская поликлиника №5»;
- Руководящих документов ФСТЭК и ФСБ России.

Выбранные необходимые мероприятия по защите ПДн отражаются в «Описании системы защиты персональных данных ММАУ «Городская поликлиника №1».

3.1. Требования по обеспечению защиты в ИСПДн «Сотрудники» и ИСПДн «Пациенты»

Для защиты от НСД в ИСПДн на рабочих станциях и серверах устанавливается средства защиты информации, обеспечивающие:

- Идентификация и аутентификация пользователей, являющихся работниками оператора;
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- Защита обратной связи при вводе аутентификационной информации
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);
- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);
- Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- Защита информации о событиях безопасности;
- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов);
- Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- Контроль состава технических средств, программного обеспечения и средств защиты информации;
- Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

3.2.Требования по организации обеспечения безопасности в ИСПДн

Регистрируемые системой защиты от НСД события безопасности на компьютерах и серверах ИСПДн должны просматриваться и анализироваться на наличие не

санкционированных действий администратором безопасности *по расписанию, указанному в пункте 2.4*.

Для эффективной защиты от вредоносных программ и вирусов на компьютерах и серверах ИСПДн периодически (*по расписанию, указанному в пункте 2.4*) должны проверятся журналы системы антивирусной защиты.

Для обеспечения защиты ИСПДн от угроз безопасности ПДн в Организации необходимо обеспечить:

- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;
- учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме);
- физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации;
- наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.
- процесса контроля за целостностью программной и информационной части, процедуры восстановления (*по расписанию, указанному в пункте 2.4*).

3.3.Порядок организации доступа к ИСПДн

Все пользователи ИСПДн должны иметь доступ к ресурсам ИСПДн только в соответствии с разрешениями, установленными в «Матрице доступа пользователей к ресурсам ИСПДн».

Организация доступа нового пользователей к ресурсам ИСПДн осуществляется следующим образом:

1. Согласование доступа пользователя к ресурсам ИСПДн и добавление пользователя в «Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн необходим для выполнения служебных (трудовых) обязанностей»;
2. Ознакомление пользователя с «Положением об обработке и защиты ПДн в Организации» и истребование с пользователя подписания «Соглашения о неразглашении ПДн»;
3. Создание учетной записи пользователя и организация доступа в соответствии с разрешениями, зафиксированными в «Матрице доступа пользователей к ресурсам ИСПДн».

При необходимости удаления доступа пользователя к ресурсам ИСПДн (в случаях увольнения сотрудника и т.д.) необходимо заблокировать (или удалить) учетную запись пользователя и откорректировать «Список лиц, доступ которых к персональным данным, обрабатываемых в ИСПДн необходим для выполнения служебных (трудовых) обязанностей».

3.4. Порядок обработки инцидентов безопасности

Порядок обработки инцидентов безопасности ПДн описан в «Инструкции по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ИСПДн».

3.5. Порядок выполнения процедур резервного копирования

Порядок процедур резервного копирования ПДн описан в «Инструкции по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ИСПДн».

4. Пользователи ИСПДн

В Организации можно выделить следующие группы пользователей ИСПДн, участвующих в обработке и хранении ПДн:

- Администратора безопасности;
- Оператора АРМ;
- Специалиста по поддержке технических средств корпоративной сети;

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в матрице доступа пользователей к ресурсам ИСПДн.

4.1 Администратор безопасности

Администратор безопасности, сотрудник Организации, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент ИСПДн.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми

пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Организации.

4.2 Оператор АРМ

Оператор АРМ, сотрудник Организации, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

4.3 Специалист по поддержке технических средств корпоративной сети

Технический специалист по обслуживанию, сотрудник Организации, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5. Требования к персоналу по обеспечению безопасности персональных данных

Все сотрудники Организации, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями положения по обработке и обеспечению безопасности персональных данных, обрабатываемых в Организации.

Сотрудники Организации, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Организации должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Организации должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам, а также бывшим сотрудникам, запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Организации, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Организации обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Организации должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных

взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Контроль за соблюдением, выше описанных требований по защите персональных данных сотрудниками Организации, возлагается на ответственного по защите информации в ИСПДн и ответственного за организацию обработки персональных данных в Организации.

6. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора защиты;
- Инструкция пользователя по эксплуатации СЗИ в ИСПДн;
- Инструкция по организации резервирования и восстановления ИСПДн, обработка инцидентов безопасности ПДн;
- Инструкция пользователей ИСПДн;

7. Ответственность сотрудников ИСПДн Организации

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками Организации – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Места размещения политики:

1. Информационные стенды в поликлинике в главном корпусе и в филиалах;
2. Официальный сайт поликлиники: **www.poliklinika5.ru**