Государственное бюджетное учреждение здравоохранения Пермского края
«Краевая клиническая стоматологическая поликлиника»

ПРИКАЗ

11.01.2021 **№ 01-02/1/2**

г. Пермь

О введении режима обработки
и защиты персональных данных
работников и пациентов ГБУЗ ПК «ККСП»

В целях обеспечения соблюдения требований законодательства о защите персональных данных, во исполнение положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить:

- Политику ГБУЗ ПК «ККСП» в отношении обработки и защиты персональных данных (далее - Политика) (Приложение № 1);
- Положение об обработке и защите персональных данных работников и пациентов ГБУЗ ПК «ККСП» (далее - Положение) (Приложение № 2);
- Форму Согласия на обработку персональных данных (Приложение №3);
- Форму Заявления об отзыве согласия на обработку персональных данных (Приложение № 4);
- Форму Заявления-согласия субъекта на получение персональных данных у третьей стороны (Приложение № 5);
- Форму Заявления-согласия субъекта на передачу его персональных данных третьей стороне (Приложение № 6);
- Форму Журнала учета передачи персональных данных (Приложение № 7);
- Форму Журнала учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных (Приложение № 8);
- План мероприятий по защите персональных данных (Приложение № 9);
- Типовой договор на поручение обработки персональных данных третьим лицам (Приложение № 10).

2. Назначить ответственными лицами за соблюдение режима обработки персональных данных:

В ГБУЗ ПК «ККСП» г.Пермь:

- Собянину Наталью Валерьевну, и.о. заведующего отделением терапевтической стоматологии № 1;
- Каширского Василия Валерьевича, заведующего отделением терапевтической стоматологии № 2;

- Попову Надежду Васильевну, заведующего отделением хирургической стоматологии;

- Першину Розу Галимзяновну, заведующего детским стоматологическим отделением;

- Беляеву Ольгу Васильевну, заведующего отделением ортопедической стоматологии;

- Зернину Ларису Валерьевну, заведующего отделением по оказанию платных медицинских услуг.

ОСП пгт.Полазна:

- Поплаухина Сергея Федоровича, заведующего обособленным структурным подразделением;

ОСП г.Добрянка:

- Дозморова Андрея Калиновича, заведующего обособленным структурным подразделением.

ОСП г.Верещагино:

- Деменеву Наталью Викторовну, заведующего обособленным структурным подразделением.

3. Обязанность по уведомлению лиц, указанных в п. 2 настоящего приказа, персонально и под подпись, возложить на сотрудников, занимающих должность: «Секретарь-машинистка» в ГБУЗ ПК «ККСП», его обособленных структурных подразделениях и структурных подразделениях:

- организовать размещение Политики на Интернет-сайте ГБУЗ ПК «ККСП»;

- ознакомить с Положением всех сотрудников ГБУЗ ПК «ККСП» и соответствующих структурных подразделений;

- ознакомить с настоящим приказом сотрудников ГБУЗ ПК «ККСП» и сотрудников соответствующих структурных подразделений.

4. Контроль исполнения приказа оставляю за собой.

Главный врач А.Ю.Новиков

Приложение № 1
к приказу от 11.01.2021
№01-02/1/2

ПОЛИТИКА
ГБУЗ ПК «ККСП»
в отношении обработки и защиты персональных данных

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом Государственного бюджетного учреждения здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника» (далее - Учреждение), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Учреждение.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Учреждением участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Учреждение становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Учреждения распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Учреждением.

1.5. Во исполнение настоящей Политики руководящим органом Учреждения утверждены следующие локальные нормативные правовые акты:

1.5.1. Положение об обработке и защите персональных данных работников и пациентов Государственного бюджетного учреждения здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника»;

1.5.2. Приказ «О порядке взаимодействия со сведениями, составляющими врачебную тайну»;

1.5.3. Перечень персональных данных, обрабатываемых в ГБУЗ ПК

«ККСП» и подлежащих защите;

1.5.4. Перечень сотрудников ГБУЗ ПК «ККСП», имеющих доступ к персональным данным работников в целях исполнения своей трудовой функции;

1.5.5. Перечень сотрудников ГБУЗ ПК «ККСП», имеющих доступ к персональным данным пациентов 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;

1.5.6. Перечень мест хранения материальных носителей персональных данных;

1.5.7. Форма Согласия на обработку персональных данных;

1.5.8. Форма Заявления об отзыве согласия на обработку персональных данных;

1.5.9. Форма Заявления-согласия субъекта на получение персональных данных у третьей стороны;

1.5.10. Форма Заявления-согласия субъекта на передачу его персональных данных третьей стороне;

1.5.11. Форма Журнала учета передачи персональных данных;

1.5.12. Форма Журнала учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных;

1.5.13. План мероприятий по защите персональных данных;

1.5.14. Типовой договор на поручение обработки персональных данных третьим лицам.

2. Основания обработки и состав персональных данных, обрабатываемых в Учреждении

2.1. Обработка ПДн в Учреждении осуществляется в связи с выполнением законодательно возложенных на Учреждение функций, определяемых:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29.07.2004 года № 98-ФЗ «О коммерческой тайне»;
- Федеральным законом от 22.10.2004 года № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федеральным законом РФ от 21.11.2011 года № 323-ФЗ «Об основах охраны здоровья граждан в РФ»;

- Федеральным законом от 25.12.2008 года № 273-ФЗ «О противодействии коррупции»;

- Федеральным законом от 02.05.2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

- Постановлением Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановлением Правительства Российской Федерации от 06.07.2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Постановлением Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказом Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Кроме того, обработка ПДн в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Учреждением своих прав и обязанностей как юридического лица.

2.2. В рамках осуществления функции по оказанию медицинских услуг ПДн обрабатываются Учреждением:

1) в ходе организации оказания медицинской помощи, 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;

2) при рассмотрении обращений граждан;

3) при обработке запросов уполномоченных органов.

При этом обрабатываются ПДн лиц, обратившихся за оказанием медицинской услуги, а также лиц, имеющих основанное на законе право обратиться в Учреждение в своих интересах или в интересах пациентов.

2.3. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Учреждение выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство в Учреждение, работников Учреждения (далее - Работники) и бывших Работников.

2.4. В связи с реализацией своих прав и в связи с соблюдением обязанностей, Учреждением обрабатываются ПДн физических лиц, являющихся контрагентами Учреждения по гражданско-правовым договорам физических лиц, ПДн которых используются для осуществления пропускного режима в занимаемых Учреждением помещениях, а также физических лиц, письменно обращающихся в Учреждение по вопросам его деятельности.

2.5. Учреждение осуществляет сбор и обработку ПДн на основании: требований законодательства РФ, согласия на обработку ПДн, а в необходимых случаях – при наличии письменного согласия субъекта ПДн.

2.6. В целях исполнения возложенных на Учреждение функций, Учреждение, в установленном порядке, вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Учреждение поручает обработку ПДн, включаются условия, обязывающие таких лиц соблюдать предусмотренные Законом о ПДн и Политикой правила обработки ПДн.

2.7. Учреждение предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

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

2.9. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения, разрушения (уничтожения) или искажения ПДн в процессе обработки.

3.2. Для обеспечения безопасности ПДн Учреждение руководствуется следующими принципами:

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

2) системность: обработка ПДн в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих значение для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения (далее - ИС) и других имеющихся в Учреждении систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень

безопасности ПДн, принимаются до начала их обработки;

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

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

8) гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Учреждения (далее - ИСПДн), а также объема и состава обрабатываемых ПДн;

9) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Учреждения (далее - СЗПДн) не дают возможности преодоления имеющихся в Учреждении систем защиты возможными нарушителями безопасности ПДн;

10) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

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

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым в Учреждении ПДн имеют лица, уполномоченные приказом Учреждения, а также лица, чьи ПДн подлежат обработке в отношении собственных ПДн.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством функции Учреждения закрепляются за соответствующими структурными подразделениями (должностными лицами) Учреждения.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Учреждения, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих Работников.

4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения. Допуск Работников к обработке ПДн производится на основании приказа, а объем ПДн, к которым предоставляется доступ, определяется как соответствующим приказом, так и положениями должностной инструкции соответствующего Работника.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами Учреждения, устанавливающими порядок обработки ПНд, включая документы, устанавливающие права и обязанности конкретных

Работников, в том числе приказ об установлении и о допуске к обработке ПДн соответствующего объема и характера.

4.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Учреждением, осуществляется в соответствии с Законом о ПДн и определяется внутренними регулятивными документами Учреждения.

5. Реализация Политики

5.1. Учреждение принимает необходимые и достаточные меры для защиты обрабатываемых ПДн от неправомерного или случайного доступа к ним, от уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними со стороны третьих лиц.

5.2. Лицо, ответственное за организацию обработки ПДн в Учреждении, определяется приказом главного врача Учреждения.

Ответственное лицо за организацию обработки ПДн в Учреждении, в частности, обязано:

1) осуществлять внутренний контроль за соблюдением в Учреждении требований нормативных правовых актов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн;

2) доводить до сведения Работников положения нормативных правовых актов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн;

3) организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.3. Учреждение осуществляет обработку ПДн как с использованием средств автоматизации, так и без использования таких средств.

5.4. При обработке ПДн без использования средств автоматизации Учреждение, в соответствии с положениями нормативных правовых актов в области обработки и защиты ПДн, реализует комплекс организационных и технических мер, обеспечивающих:

1) обособление ПДн от информации, не содержащей ПДн;

2) раздельную обработку и хранение каждой категории ПДн (фиксация на отдельных материальных носителях ПДн, цели обработки которых заведомо несовместимы);

3) соответствие типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн, установленным требованиям;

4) соблюдение установленных требований при ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн в помещения, занимаемые Учреждением, или в иных аналогичных целях;

5) сохранность материальных носителей ПДн;

6) условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых

осуществляется в различных целях;

7) надлежащее уточнение, уничтожение или обезличивание ПДн.

5.5. В соответствии с требованиями нормативных правовых актов в области обработки и защиты ПДн обработки ПДн с использованием средств автоматизации в Учреждении создаются ИСПДн.

Все ИСПДн проходят периодическую классификацию и аттестацию в соответствии с требованиями нормативных правовых актов в области обеспечения безопасности ПДн.

Для каждой ИСПДн формируется модель угроз безопасности ПДн и на ее основе проводятся мероприятия по обеспечению безопасности информации в соответствии с требованиями, предъявляемыми к установленному классу ИСПДн.

Пересмотр моделей угроз для каждой ИСПДн осуществляется:

а) в плановом порядке для существующих ИСПДн - ежегодно;

б) в случае существенных изменений в инфраструктуре или порядке обработки ПДн в ИСПДн - в течение трех месяцев с даты фиксации изменений;

в) в случае создания новой ИСПДн (выделения части из существующей ИСПДн) - в течение одного месяца с даты создания (выделения) ИСПДн.

5.6. Обработка ПДн в Учреждении с использованием средств автоматизации ведется только в ИСПДн. В Учреждении запрещается обработка ПДн с целями, не соответствующими целям создания ИСПДн, эксплуатация ИСПДн в составе, отличном от указанного при создании ИСПДн.

5.7. Ввод в эксплуатацию ИСПДн оформляется актом ввода в эксплуатацию и сопровождается аттестацией ИСПДн или декларированием соответствия ИСПДн требованиям по безопасности ПДн.

5.8. В целях обеспечения управления информационной безопасностью ПДн в Учреждении создается СЗПДн.

Объектами защиты СЗПДн являются информация, обрабатываемая Учреждением и содержащая ПДн, а также инфраструктура, содержащая и поддерживающая указанную информацию.

5.9. СЗПДн реализуется комплексом правовых, режимных, организационных и программно-технических мер, которые включают:

1) подготовку внутренних регулятивных документов Учреждения по вопросам обработки и защиты ПДн, контроль за исполнением в Учреждении требований нормативных правовых актов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн, а также внесение соответствующих изменений в имеющиеся внутренние регулятивные документы;

2) оформление письменных обязательств Работников о неразглашении ПДн;

3) доведение до сведения Работников информации об установленных законодательством Российской Федерации санкциях за нарушения, связанные с обработкой и защитой ПДн;

4) обеспечение наличия в положениях о структурных подразделениях

Учреждения и должностных обязанностях Работников требований по соблюдению установленного порядка обработки и защиты ПДн;

5) разработку и введение в действие внутренних регулятивных документов Учреждения по обеспечению информационной безопасности ИСПДн;

6) регламентацию процедур создания и осуществление документирования действующих инженерных и информационных систем, программных комплексов, порядка внесения в них изменений и своевременной актуализации эксплуатационной документации;

7) ознакомление Работников с положениями нормативных правовых актов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн, а также обучение Работников правилам обработки и защиты ПДн;

8) проведение мероприятий по регламентации, установлению, поддержанию и осуществлению контроля за состоянием:

а) физической охраны, контрольно-пропускного режима, перемещением технических средств и носителей информации;

б) защиты технологических процессов, информационных ресурсов, информации и поддерживающей их инфраструктуры от угроз техногенного характера и внешних неинформационных воздействий;

9) регламентацию обработки ПДн, в том числе хранения и передачи информации как внутри Учреждения, так и при взаимодействии с контрагентами Учреждения, государственными органами и организациями, обращения с документами (включая электронные документы) и носителями, порядка их учета, хранения и уничтожения;

10) установление правил доступа на объекты, в помещения, в ИС, применению в этих целях систем охраны и управления доступом;

11) формирование участков (выделение в отдельные VLAN (виртуальные локальные компьютерные сети) технических средств) администрирования безопасности, мониторинга и аудита, управления доступом к защищаемым ресурсам;

12) организацию технического оснащения объектов и ИСПДн в соответствии с существующими требованиями к информационной безопасности;

13) формирование условий и технологических процессов обработки, хранения и передачи информации в Учреждении (включая условия хранения документов в архивах), обеспечивающих реализацию требований нормативных правовых актов, методических документов уполномоченных государственных органов и внутренних регулятивных документов Учреждения в области обработки и защиты ПДн;

14) установление полномочий пользователей и форм представления информации пользователям ИСПДн;

15) организацию непрерывного процесса контроля (мониторинга) событий безопасности для своевременного выявления и пресечения попыток несанкционированного доступа к защищаемой информации;

16) организацию необходимых мероприятий с Работниками, обучение

Работников требованиям информационной безопасности;

17) осуществление контроля эффективности организационных мер защиты;

18) разработку защитных технических решений:

а) при стратегическом планировании архитектуры ИС;

б) выборе технических средств обработки информации;

в) разработке и (или) приобретении программного обеспечения;

19) применение следующих компонентов программно-технических мер защиты:

а) защищенных средств (систем) обработки информации, содержащей ПДн;

б) системы криптографической защиты информации при ее передаче по каналам связи;

в) межсетевых экранов для логического разделения подсетей и защиты от несанкционированного доступа из внешних (открытых) информационных систем;

г) аппаратных и программных средств защиты и контроля, устройств, технических систем и средств, используемых для обеспечения информационной безопасности, в том числе для обнаружения и нейтрализации попыток несанкционированного доступа к информации.

5.10. Для всех критичных в отношении обеспечения целостности и доступности ПДн функций ИСПДн разрабатываются соответствующие планы обеспечения непрерывной работы и восстановления при авариях и стихийных бедствиях, которые не реже одного раза в квартал проходят актуализацию. Работники проходят обучение необходимым действиям по обеспечению целостности и доступности ПДн в нештатных ситуациях.

6. Основные мероприятия по обеспечению безопасности персональных данных

6.1. Мероприятия по защите ПДн реализуются в Учреждении в следующих направлениях:

1) предотвращение утечки информации, содержащей ПДн, по техническим каналам связи и иными способами;

2) предотвращение несанкционированного доступа к содержащей ПДн информации, специальных воздействий на такую информацию (носители информации) в целях ее сбора, уничтожения, искажения и блокирования доступа к ней;

3) защита от вредоносных программ;

4) обеспечение безопасного межсетевого взаимодействия;

5) обеспечение безопасного доступа к сетям международного информационного обмена;

6) анализ защищенности ИСПДн;

7) обеспечение защиты информации с использованием шифровальных (криптографических) средств при передаче ПДн по каналам связи;

8) обнаружение вторжений и компьютерных атак;

9) осуществления контроля за реализацией системы защиты ПДн.

6.2. Мероприятия по обеспечению безопасности ПДн включают в себя:

1) реализацию разрешительной системы допуска пользователей (Работников) к информационным ресурсам ИС и связанным с их использованием работам, документам;

2) разграничение доступа пользователей ИСПДн и обслуживающих ИСПДн Работников к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

3) регистрацию действий пользователей и обслуживающих ИСПДн Работников, контроль несанкционированного доступа и действий пользователей и обслуживающих Работников, а также третьих лиц;

4) использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

5) предотвращение внедрения в ИС вредоносных программ и программных закладок, анализ принимаемой по информационно-телекоммуникационным сетям (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов;

6) ограничение доступа к техническим средствам, позволяющим осуществлять обработку ПДн;

7) размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

8) организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн;

9) учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

10) резервирование технических средств, дублирование массивов и носителей информации;

11) реализацию требований по безопасному межсетевому взаимодействию ИС;

12) использование защищенных каналов связи, защита информации при ее передаче по каналам связи;

13) межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИС;

14) обнаружение вторжений в ИС, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности ПДн;

15) периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на ИС;

16) активный аудит безопасности ИС на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;

17) анализ защищенности ИС с применением специализированных программных средств (сканеров безопасности);

18) централизованное управление системой защиты ПДн в ИС.

6.3. В целях организации работ по обеспечению информационной безопасности ПДн в Учреждении определяются структурные подразделения,

на которые возлагаются задачи:

1) по классификации, паспортизации и аттестации ИСПДн;

2) организации разработки модели угроз для каждой ИСПДн;

3) организации разработки технического проекта системы защиты информации для каждой ИСПДн;

4) закупке, установки, эксплуатации и администрирования средств защиты информации;

5) организации разрешительной системы допуска к информации, содержащей ПДн и разработке внутренних регулятивных документов Учреждения по этому вопросу;

6) организации реагирования на события безопасности;

7) контролю состояния системы защиты информации и планирования соответствующих мероприятий.

6.4. С целью поддержания состояния защиты ПДн на надлежащем уровне в Учреждении осуществляется внутренний контроль за эффективностью системы защиты ПДн и соответствием порядка и условий обработки и защиты ПДн установленным требованиям.

Внутренний контроль включает:

1) мониторинг состояния технических и программных средств, входящих в состав СЗПДн;

2) контроль соблюдения требований по обеспечению безопасности ПДн (требований нормативных правовых актов и внутренних регулятивных документов в области обработки и защиты ПДн, требований договоров).

6.5. В целях осуществления внутреннего контроля в Учреждении проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Учреждении либо комиссией, образуемой главным врачом Учреждения.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается главному врачу Учреждения.

Приложение № 2
к приказу от 11.01.2021
№01-02/1/2

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников и пациентов Государственного бюджетного учреждения здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника»

I. Общие положения

1.1. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных субъектов персональных данных учреждения здравоохранения (работников и пациентов), а также ведения их личных дел, медицинских карт.

1.2. Цель настоящего Положения – обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных сотрудников, пациентов, контрагентов, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Настоящее Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 29.07.2004 года № 98-ФЗ «О коммерческой тайне»;
- Федеральным законом от 22.10.2004 года № 125-ФЗ «Об архивном деле в Российской Федерации»;
- Федеральным законом РФ от 21.11.2011 года № 323-ФЗ «Об основах охраны здоровья граждан в РФ»;
- Федеральным законом от 25.12.2008 года № 273-ФЗ «О противодействии коррупции»;
- Федеральным законом от 02.05.2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Постановлением Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановлением Правительства Российской Федерации от 06.07.2008 года № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

- Постановлением Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Приказом Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

1.4. В настоящем Положении используются следующие термины и определения:

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, биометрические данные, другая информация.

Оператор – Государственное бюджетное учреждение здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника» (далее по тексту – ГБУЗ ПК «ККСП»). К понятию «Оператор» также относятся обособленные структурные подразделения ГБУЗ ПК «ККСП».

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

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

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

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Информационная система персональных данных (ИСПДН) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного

государства, иностранному физическому лицу или иностранному юридическому лицу.

II. Принципы и условия обработки персональных данных

2.1 Обработка персональных данных должна осуществляться с соблюдением следующих принципов:

2.1.1 Обработке подлежат только персональные данные, которые отвечают конкретным, заранее определенным и законным целям их обработки (обеспечение трудового договора, содействие работникам в трудоустройстве, обучении и продвижении по службе, обеспечение личной безопасности, обследование, наблюдение и лечение пациентов, обеспечение сохранности имущества оператора, работника, пациента и третьих лиц, оформление гражданско-правовых договоров и др.).

2.1.2 Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными нормативными правовыми актами, в том числе локальными.

2.1.3 При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность.

2.1.4 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

2.1.5 Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2 Обработка персональных данных допускается в следующих случаях:

2.2.1 Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в федеральном законе.

В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных.

2.2.2 Обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащего исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

2.2.3 Обработка персональных данных необходима для исполнения договора, стороной которого, выгодоприобретателем или поручителем является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или по инициативе оператора или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

2.2.4 Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

2.2.5 Обработка персональных данных 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 персональных данных;

2.2.6 Обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

2.2.7 Осуществляется обработка персональных данных, которые стали общедоступными в связи с действиями субъекта персональных данных;

2.3 Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, когда:

2.3.1 субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

2.3.2 персональные данные сделаны общедоступными в связи с действиями субъекта персональных данных;

2.3.3 обработка осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, а также в соответствии с иными положениями законодательства;

2.3.4 обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, либо для защиты жизни, здоровья или иных жизненно важных интересов других лиц, а получение согласия на обработку персональных данных от субъекта персональных данных получить невозможно;

2.3.5 обработка персональных данных 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;

2.3.6 обработка персональных данных осуществляется в соответствии с законодательством, регулирующим вопросы страхования граждан для оказания им медицинской помощи;

2.3.7 в других случаях, предусмотренных федеральными законами.

2.4 Сведения, которые характеризуют физиологические и биологические особенности человека, (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами

2.5 Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

2.6 При сборе персональных данных оператор обязан предоставить (за исключением случаев, предусмотренных федеральными законами) субъекту персональных данных по его просьбе следующую информацию:

2.6.1 подтверждение факта обработки персональных данных оператором;

2.6.2 правовые основания и цели обработки персональных данных;

2.6.3 цели и применяемые оператором способы обработки персональных данных;

2.6.4 наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

2.6.5 обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

2.6.6 сроки обработки персональных данных, в том числе сроки их хранения;

2.6.7 порядок осуществления субъектом персональных данных прав, предусмотренных соответствующими федеральными законами;

2.6.8 информацию об осуществленной или о предполагаемой трансграничной передаче данных;

2.6.9 наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена такому лицу;

2.7 Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

2.8 Информация о персональных данных предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников (медицинских карт для пациентов), которые хранятся в личном деле в отделе кадров (регистратуре/архиве). Если персональные данные субъекта

возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом.

В письменном уведомлении оператор должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

2.9 При поступлении на работу работник представляет сотрудникам отдела кадров следующие документы, содержащие персональные данные:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о регистрации индивидуального налогового номера (ИНН);
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- документ о прохождении медицинского осмотра в целях охраны здоровья населения, предупреждения возникновения и распространения заболеваний.

2.10 При оказании медицинских услуг пациент предоставляет следующие документы, содержащие персональные данные:

- паспорт или иной документ, удостоверяющий личность, гражданство;
- полис ОМС;
- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
- в отдельных случаях с учетом специфики обследования в учреждении здравоохранения действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.

2.11 Запрещается требовать от лица, поступающего на работу (или прием), документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

2.12 При заключении трудового договора и/или в ходе трудовой деятельности может возникнуть необходимость в предоставлении работником следующих документов, содержащих персональные данные:

- о возрасте детей;
- об инвалидности;
- о донорстве;
- о составе семьи;
- о необходимости ухода за больным членом семьи;
- прочие.

2.13 После того, как будет принято решение о приеме работника на работу, а также впоследствии в процессе трудовой деятельности, к документам, содержащим персональные данные субъекта персональных данных, также будут относиться:

- трудовой договор;
- приказ о приеме на работу;
- приказы о поощрениях и взысканиях;
- медицинский осмотр сотрудника при приеме на работу (флюорограмма грудной клетки, анализ крови на RW, ВИЧ, гепатиты и др.);
- приказы, связанные с аттестацией, повышением квалификации сотрудников и др.;
- карточка унифицированной формы Т-2, утвержденная постановлением Госкомстата России от 05.01.04 №1;
- другие документы в соответствии с законодательством Российской Федерации.

2.14 В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

2.15 К числу потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, областных и муниципальных органов управления. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

III. Состав персональных данных

3.1. В состав персональных данных субъектов Оператора входит:

3.1.1. Фамилия, имя, отчество;
3.1.2. Дата рождения;
3.1.3. Место рождения;
3.1.4. Адрес;
3.1.5. Семейное, социальное и имущественное положение;
3.1.6. Образование и специальность;
3.1.7. Профессия;
3.1.8. Должность;
3.1.9. Заработная плата (оклад, премии, надбавки);
3.1.10. Номера банковских расчетных счетов;
3.1.11. Сведения о социальных льготах;
3.1.12. Паспортные данные;
3.1.13. ИНН;

3.1.14. Информация о воинской обязанности;
3.1.15. Данные страхового полиса обязательного медицинского страхования (ОМС);
3.1.16. Данные страхового полиса обязательного пенсионного страхования (СНИЛС);
3.1.17. Трудовой стаж;
3.1.18. Данные о предыдущих местах работы;
3.1.19. Фотографии;
3.1.20. Адрес электронной почты;
3.1.21. Телефон (домашний, сотовый);
3.1.22. Фамилия, имя, отчество дата рождения детей;
3.1.23. Фамилия, имя, отчество, год рождения членов семьи и ближайших родственников;
3.1.24. Данные о состоянии здоровья и сотрудников и пациентов и оказанных им медицинских услугах.

3.2. В ГБУЗ ПК «ККСП» создаются и хранятся следующие документы, содержащие данные о субъектах персональных данных:
3.2.1. Унифицированная форма Т-2 «Личная карточка работника»;
3.2.2. Личное дело работника;
3.2.3. Докладные записки, объяснительные записки нарушителей трудовой дисциплины;
3.2.4. Книга учета принятых и уволенных работников;
3.2.5. Трудовые книжки;
3.2.6. Резюме соискателя;
3.2.7. Заявления работника;
3.2.8. Договоры на оказание услуг сторонними организациями;
3.2.9. Списки работников, подлежащих периодическому медицинскому осмотру;
3.2.10. Направления на плановые медосмотры;
3.2.11. Направления на обучение и курсы повышения квалификации;
3.2.12. Командировочные удостоверения;
3.2.13. Больничные листы;
3.2.14. Табеля учета рабочего времени;
3.2.15. Медицинские карты пациентов и сотрудников.

IV. Цель обработки персональных данных

4.1. Целью обработки персональных данных субъектов является соблюдение трудового законодательства РФ, законодательства РФ об охране труда и техники безопасности, законодательства РФ об охране здоровья, о коммерческой тайне, о противодействии коррупции, заключение и исполнение договоров, стороной которых являются субъекты персональных данных, организация многократного и однократного пропуска субъекта персональных данных на территорию ГБУЗ ПК «ККСП», зачисление заработной платы работников на банковские карты, размещение информации о руководителях и медперсонале ГБУЗ ПК «ККСП» на официальном сайте Оператора в соответствии с требованиями законодательства.

V. Сбор, обработка, хранение и защита персональных данных

5.1. Порядок получения (сбора) персональных данных:

5.1.1. Все персональные данные субъекта следует получать у него лично с его письменного согласия, кроме случаев, определенных в п. 5.1.3. и 5.1.6. настоящего Положения и иных случаях, предусмотренных законами.

5.1.2. Согласие субъекта на обработку персональных данных действует в течение неопределенного срока, пока сохраняется цель обработки персональных данных, если иное не предусмотрено законом, либо до отзыва согласия на обработку (для пациентов).

5.1.3. Если персональные данные субъекта возможно получить только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Третье лицо, предоставляющее персональные данные субъекта, должно обладать согласием субъекта на передачу персональных данных Оператору. Оператор обязан получить подтверждение от третьего лица, передающего персональные данные субъекта персональных данных о том, что персональные данные передаются с согласия субъекта. Оператор при взаимодействии с третьими лицами обязан заключить с ними соглашение (статья договора) о конфиденциальности информации, касающейся персональных данных субъектов.

5.1.4. Оператор обязан сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

5.1.5. Обработка персональных данных субъектов без их согласия осуществляется в следующих случаях:

5.1.5.1. Персональные данные являются общедоступными.

5.1.5.2. По требованию полномочных органов государственной власти в случаях, предусмотренных федеральным законом.

5.1.5.3. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия Оператора.

5.1.5.4. Обработка персональных данных осуществляется в целях заключения и исполнения договора, одной из сторон которого является субъект персональных данных.

5.1.5.5. Обработка персональных данных осуществляется для статистических целей при условии обязательного обезличивания персональных данных.

5.1.5.6. В иных случаях, предусмотренных законом.

5.1.6. Оператор не обрабатывает персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

5.2. Порядок обработки и хранения персональных данных:

5.2.1. Субъект персональных данных предоставляет Оператору письменное согласие на обработку своих персональных данных. Затем предоставляет сотруднику Оператора, уполномоченному вести обработку персональных данных, те данные, которые необходимы для достижения цели их обработки.

5.2.2. На основании полученной информации уполномоченный сотрудник Оператора проверяет наличие данного субъекта в информационной системе. Если субъект не зарегистрирован в информационной системе, то операционный сотрудник заносит в систему полную информацию о нем. В случае наличия информации о субъекте в информационной системе – сверяет данные с ранее предоставленными и при необходимости вносит соответствующие изменения.

5.2.3. Своевременно, в срок, не превышающий 5 (Пяти) рабочих дней, субъект персональных данных обязан лично или через своего законного представителя сообщать работнику, ответственному за сбор информации, об изменениях своих персональных данных с предоставлением соответствующих документов.

5.2.4. Оператор прекращает обработку персональных данных в случае исчерпания цели обработки персональных данных, увольнения субъекта персональных данных, если иное не предусмотрено законом.

5.2.5. Персональные данные субъектов хранятся на бумажных носителях в помещении отдела кадров (регистратуре). Для этого используются специально оборудованные шкафы и/или сейфы. Личные дела уволенных (прошедших обследование, лечение) субъектов персональных данных хранятся в архиве ГБУЗ ПК «ККСП».

5.2.6. Сведения о начислении и выплате заработной платы работникам ГБУЗ ПК «ККСП» хранятся на бумажных носителях в помещениях экономического отдела и отдела бухгалтерского учета. По истечении сроков хранения, установленных законодательством РФ, данные сведения передаются в архив ГБУЗ ПК «ККСП».

5.2.7. Конкретные обязанности по ведению, хранению личных дел субъектов персональных данных, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные субъектов персональных данных, возлагаются на работников отдела кадров, а по хранению личных дел уволенных (обследованных, пролеченных) субъектов – на работников архива и закрепляются в должностных инструкциях соответствующих работников.

5.2.8. Персональные данные субъектов персональных данных хранятся в течение срока, определенного п. 5.1.2. настоящего Положения, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

5.2.9. Сведения о субъектах ПДн Оператора хранятся также на электронных носителях – в базах данных «Федеральный регистр медицинских работников (ГАУЗ «МИАЦ)», Перечень ЛП 1.4;1.4.2 (передача сведений в пенсионный фонд). Система эл. документооборот Клиент СЭД, «Парус: Зарплата», «СБИС++. Электронная отчетность» (передача сведений в налоговую инспекцию и пенсионный фонд), «ПДСПУ 2010» (передача сведений в пенсионный фонд), Учет льготных рецептов в ЛПУ (Lrecept), «1С: Предприятие. Бухгалтерия для бюджетных учреждений», базах лабораторных исследований диагностической, клинико-диагностической и бактериологических лабораторий, базе ВИЧ-инфицированных эпидемиологического отдела, ИАС ПК «Промед-веб».

5.2.10. При получении сведений, составляющих персональные данные субъектов персональных данных, заинтересованные лица имеют право получать

только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

5.2.11. Использование и хранение биометрических персональных данных вне информационных систем персональных данных может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

5.3. Защита информации о персональных данных:

5.3.1. Под защитой персональных данных субъекта понимается комплекс мер (организационно-распорядительных, технических, юридических), направленных на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных субъектов, а также от иных неправомерных действий.

5.3.2. Защита персональных данных субъекта осуществляется за счет Оператора в порядке, установленном соответствующими федеральными законами и внутренними организационными документами Оператора.

5.3.3. Сотрудники ГБУЗ ПК «ККСП», имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

5.3.4 Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения установленных Правительством Российской Федерации уровней защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.3.5. Программисты (техники) ОМО обеспечивают следующие меры по защите хранящейся на сервере информации:

- установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- организация в отдельном сегменте сети всех компьютеров пользователей и серверов с ограниченным доступом из локальной сети ГБУЗ ПК «ККСП»;

- организация контроля технического состояния серверов и уровней защиты информации;

- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- проведение регулярного резервного копирования информации;

- ведение аудита действий пользователей, своевременное обнаружение фактов несанкционированного доступа к информации и принятие мер;

5.3.6. Сотрудники ГБУЗ ПК «ККСП», имеющие доступ к персональным данным, при пользовании доступом в сеть Интернет обязаны принимать максимальные меры по обеспечению безопасности:

- установить и использовать антивирусное ПО (с обновлением баз вирусов);

- установить и использовать брэндмауэр;

- устанавливать обновления для операционной системы.

5.3.7. Защита персональных данных работников и пациентов в ГБУЗ ПК «ККСП» возлагается на:

- главного врача учреждения;
- зам. главного врача по организационно-методическим вопросам;
- зам. главного врача по медицинской части;
- зам. главного врача по экономике;
- зам. главного врача по АХЧ;
- главного бухгалтера;
- работников отдела кадров (ведение трудовых книжек, личных карточек формы Т-2, личных дел);
- юрисконсульта;
- работников бухгалтерии (ведение документации по учету труда и его оплате);
- работников экономической службы;
- инженера по охране труда;
- программистов;
- председателя совета трудового коллектива;
- руководителей структурных подразделений;
- главную медицинскую сестру;
- старших медицинских сестер отделений;
- врачей и средний медицинский персонал.

VI. Передача персональных данных

6.1. При передаче персональных данных субъектов персональных данных сотрудники ГБУЗ ПК «ККСП», имеющие доступ к персональным данным, должны соблюдать следующие требования:

6.1.1. Не раскрывать третьим лицам персональные данные и не раскрывать соответствующую информацию третьим лицам без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.1.2. Поручать обработку персональных данных другому лицу только с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

6.1.3. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

6.1.4. Предупредить лиц, получающих персональные данные 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.

6.1.5. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

6.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением сведений, относящихся к вопросу о возможности выполнения работником трудовой функции, и сведений, которые необходимо обработать в целях охраны здоровья населения, предупреждения возникновения и распространения заболеваний;

6.1.7. Передавать персональные данные работника представителю субъекта персональных данных в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанным представителем его функций.

6.1.8 Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

6.2. Все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившим запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается какая именно информация была передана.

VII. Блокировка, обезличивание, уничтожение персональных данных

7.1. Порядок блокировки и разблокировки персональных данных:

7.1.1. Блокировка персональных данных субъектов осуществляется с письменного заявления субъекта персональных данных.

7.1.2. Блокировка персональных данных подразумевает:

7.1.2.1. Запрет редактирования персональных данных.

7.1.2.2. Запрет распространения персональных данных любыми средствами (электронная почта, сотовая связь, материальные носители).

7.1.2.3. Запрет использования персональных данных в массовых рассылках (SMS, электронная почта, почта).

7.1.2.4. Запрет открытия банковских счетов.

7.1.2.5. Изъятие бумажных документов, относящихся к субъекту персональных данных и содержащих его персональные данные из внутреннего документооборота Оператора и запрет их использования.

7.1.3. Блокировка персональных данных субъекта может быть временно снята, если это требуется для соблюдения законодательства.

7.1.4. Разблокировка персональных данных субъекта осуществляется с его письменного согласия или заявления.

7.1.5. Повторное согласие субъекта персональных данных на обработку его данных влечет разблокирование его персональных данных.

7.2. Порядок обезличивания и уничтожения персональных данных:

7.2.1. Обезличивание персональных данных субъекта происходит по письменному заявлению субъекта персональных данных, при условии, что все договорные отношения завершены и от даты окончания последнего договора прошло не менее 5 (Пяти) лет.

7.2.2. При обезличивании персональные данные в информационных системах заменяются набором символов, по которому невозможно определить принадлежность персональных данных к конкретному субъекту.

7.2.3. Бумажные носители документов при обезличивании персональных данных уничтожаются. В случае невозможности уничтожения бумажных носителей, содержащих персональные данные как обезличиваемого субъекта, так и других субъектов персональных данных, персональные данные уничтожаются посредством механического устройства для измельчения бумаги.

7.2.4. Операция обезличивания персональных данных субъекта необратима.

7.2.5. Оператор обязан обеспечить конфиденциальность в отношении персональных данных при необходимости проведения испытаний информационных систем на территории разработчика и произвести обезличивание персональных данных в передаваемых разработчику информационных системах.

7.2.6. Уничтожение персональных данных субъекта подразумевает прекращение какого-либо доступа к персональным данным субъекта.

7.2.7. При уничтожении персональных данных субъекта работники Оператора не могут получить доступ к персональным данным субъекта в информационных системах.

7.2.8. Бумажные носители при уничтожении персональных данных уничтожаются, персональные данные в информационных системах обезличиваются. Персональные данные восстановлению не подлежат.

7.2.9. Операция уничтожения персональных данных необратима.

VIII. Права и обязанности субъекта персональных данных

8.1. Субъект персональных данных имеет право на получение сведений о наличии у оператора своих персональных данных, целях и способах их обработки. Сведения должны быть предоставлены субъекту персональных данных оператором при обращении либо при получении запроса субъекта персональных данных или его представителя в доступной форме, и в них не должны содержаться персональные

данные, относящиеся к другим субъектам персональных данных. Право субъекта персональных данных на доступ к своим персональным данным может быть ограничено только в случаях, предусмотренных законом.

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

8.3. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор, http://www. rsoc.ru) и территориальный орган Роскомнадзора по Пермскому краю.

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

8.5 В целях обеспечения достоверности персональных данных субъект обязан:

8.5.1 При приеме на работу (к врачу) предоставить оператору необходимые и достоверные персональные данные.

8.5.2 В случае представления работником учреждению при заключении трудового договора подложных документов, трудовой договор может быть расторгнут по инициативе работодателя на основании ч. 11 статьи 81 Трудового Кодекса Российской Федерации.

8.5.3 Своевременно, в срок, не превышающий 5 (Пять) рабочих дней, сообщать учреждению об изменении своих персональных данных.

8.6 Оператор обязан:

8.6.1 Осуществлять защиту персональных данных субъектов.

8.6.2 Обеспечить хранение первичной документации по учету труда и его оплаты (документы по учету кадров, по учету и использованию рабочего времени, по оплате труда, медицинская документация и др.) При этом персональные данные не должны храниться дольше, чем это необходимо для достижения целей и выполнения задач, для которых они собирались, или дольше, чем это требуется в интересах субъектов персональных данных.

8.6.3 Заполнение документации, содержащей персональные данные субъекта, осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.04 №1.

8.6.4 По письменному заявлению субъекта персональных данных не позднее трех рабочих дней со дня подачи этого заявления выдать копии документов, связанных с работой и учебой (копии приказа о приеме на работу, приказов о переводах, приказа об увольнении с работы); выписки из трудовой книжки; справки о заработной плате, о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование, о периоде работы у данного оператора и

другие. Копии документов, связанных с работой или учебой, должны быть заверены надлежащим образом и предоставляться субъекту безвозмездно.

IX. Обязанности оператора

9.1 Учреждение при обработке персональных данных обязано принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий. Защита персональных данных от неправомерного их использования или утраты должна быть обеспечена учреждением за счет его средств, в порядке, установленном федеральным законом «О персональных данных».

9.2 Учреждение обязано в порядке, предусмотренном федеральным законом «О персональных данных», сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту, а также предоставить возможность ознакомления с ними при обращении субъекта либо в течение 30-ти рабочих дней с даты получения запроса. В случае отказа в предоставлении информации оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на основание для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса.

9.3 В случае выявления неправомерной обработки персональных данных, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.

9.4 Оператор должен обеспечить хранение первичной документации по учету труда и его оплаты (документы по учету кадров, по учету и использованию рабочего времени, по оплате труда, медицинская документация и др.) При этом персональные данные не должны храниться дольше, чем это необходимо для выполнения задач, для которых они собирались, или дольше, чем это требуется в интересах субъектов персональных данных.

9.5 Заполнение документации, содержащей персональные данные субъекта, осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.2004 №1.

9.6 При обращении (получении запроса) субъекта или его представителя выдать копии документов (копии приказа о приеме на работу, приказов о переводах, приказа об увольнении с работы); выписки из трудовой книжки; справки о заработной плате, о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование, о периоде работы у данного оператора и другие). Копии документов, должны быть заверены надлежащим образом и предоставляться субъекту безвозмездно.

9.7 Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

9.8 Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных.

X. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъекта

10.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут предусмотренную законодательством Российской Федерации (дисциплинарную, гражданскую, административную и уголовную) ответственность.

10.2 Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

XI. Заключительные положения

11.1. Настоящее Положение вступает в силу с момента его утверждения главным врачом медицинского учреждения.

11.2. Настоящее Положение доводится до сведения всех субъектов персональных данных - работников медицинского учреждения.

Согласовано:
Юрисконсульт _____

«____» _____20__г.

Государственное бюджетное учреждение здравоохранения Пермского края
«Краевая клиническая стоматологическая поликлиника»

ПРИКАЗ

11.01.2021 **№ 01-02/1/2**

г. Пермь

О введении режима обработки
и защиты персональных данных
работников и пациентов ГБУЗ ПК «ККСП»

В целях обеспечения соблюдения требований законодательства о защите персональных данных, во исполнение положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить:

- Политику ГБУЗ ПК «ККСП» в отношении обработки и защиты персональных данных (далее - Политика) (Приложение № 1);
- Положение об обработке и защите персональных данных работников и пациентов ГБУЗ ПК «ККСП» (далее - Положение) (Приложение № 2);
- Форму Согласия на обработку персональных данных (Приложение №3);
- Форму Заявления об отзыве согласия на обработку персональных данных (Приложение № 4);
- Форму Заявления-согласия субъекта на получение персональных данных у третьей стороны (Приложение № 5);
- Форму Заявления-согласия субъекта на передачу его персональных данных третьей стороне (Приложение № 6);
- Форму Журнала учета передачи персональных данных (Приложение № 7);
- Форму Журнала учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных (Приложение № 8);
- План мероприятий по защите персональных данных (Приложение № 9);
- Типовой договор на поручение обработки персональных данных третьим лицам (Приложение № 10).

2. Назначить ответственными лицами за соблюдение режима обработки персональных данных:

В ГБУЗ ПК «ККСП» г.Пермь:

- Собянину Наталью Валерьевну, и.о. заведующего отделением терапевтической стоматологии № 1;
- Каширского Василия Валерьевича, заведующего отделением терапевтической стоматологии № 2;

- Попову Надежду Васильевну, заведующего отделением хирургической стоматологии;

- Першину Розу Галимзяновну, заведующего детским стоматологическим отделением;

- Беляеву Ольгу Васильевну, заведующего отделением ортопедической стоматологии;

- Зернину Ларису Валерьевну, заведующего отделением по оказанию платных медицинских услуг.

ОСП пгт.Полазна:

- Поплаухина Сергея Федоровича, заведующего обособленным структурным подразделением;

ОСП г.Добрянка:

- Дозморова Андрея Калиновича, заведующего обособленным структурным подразделением.

ОСП г.Верещагино:

- Деменеву Наталью Викторовну, заведующего обособленным структурным подразделением.

3. Обязанность по уведомлению лиц, указанных в п. 2 настоящего приказа, персонально и под подпись, возложить на сотрудников, занимающих должность: «Секретарь-машинистка» в ГБУЗ ПК «ККСП», его обособленных структурных подразделениях и структурных подразделениях:

- организовать размещение Политики на Интернет-сайте ГБУЗ ПК «ККСП»;

- ознакомить с Положением всех сотрудников ГБУЗ ПК «ККСП» и соответствующих структурных подразделений;

- ознакомить с настоящим приказом сотрудников ГБУЗ ПК «ККСП» и сотрудников соответствующих структурных подразделений.

4. Контроль исполнения приказа оставляю за собой.

Главный врач А.Ю.Новиков

Приложение № 3
к приказу от 11.01.2021
№01-02/1/2

СОГЛАСИЕ
на обработку персональных данных

Я,
нижеподписавшийся_____,
(Ф.И.О. полностью)
проживающий по адресу_____
_____,
(по месту регистрации)
паспорт _____,
(серия, номер, дата выдачи
_____
_____,
наименование выдавшего органа)
в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных», даю свое согласие на обработку моих персональных данных Государственным бюджетным учреждением здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника» (ГБУЗ ПК «ККСП»), находящимся по адресу: г. Пермь, ул. Братьев Игнатовых, 4 (далее - Оператор), а также его обособленным структурным подразделениям, в том случае, если оказание медицинских услуг производится по адресу местонахождения такого ОСП, в целях предоставления медицинской услуги при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну. Мои персональные данные включают: страховой номер индивидуального лицевого счета, фамилию, имя, отчество, дата рождения, код, наименование и дату выдачи документа, удостоверяющего личность, адрес места регистрации и фактический адрес, а также информацию о документах на получение набора социальных услуг (серия и номер документа, код установленной льготы, период действия установленной льготы) контактные телефон(ы), реквизиты полиса ОМС (ДМС), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС).

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных.

Оператор имеет право во исполнение своих обязательств на обмен (прием и передачу) моими персональными данными с медицинскими организациями,

органам исполнительной власти, государственным структурам, а так же в порядке установленном действующим законодательством с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будет осуществляться лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов (двадцать пять лет - для стационара, пять лет – для поликлиники).

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

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной 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.

Настоящее согласие дано мной «_ _ __»_____ 20___г. и действует бессрочно.

Контактный телефон(ы) _____
Почтовый адрес _____

Подпись субъекта персональных данных _____

Приложение № 4
к приказу от 11.01.2021
№01-02/1/2

Главному врачу ГБУЗ ПК «ККСП»
г. Пермь, ул. Братьев Игнатовых, д.4
А.Ю.Новикову

_____
(фамилия, имя, отчество обратившегося)
_____
_____
(адрес места жительства)
_____
_____
(сведения о документе, удостоверяющим личность)
_____
_____
_____

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с _____.
(указать причину)

"__" _____ 20__ г.

_____ _____
(подпись) (расшифровка подписи)

Приложение № 5
к приказу от 11.01.2021
№01-02/1/2

Главному врачу ГБУЗ ПК «ККСП»
г. Пермь, ул. Братьев Игнатовых, д.4
А.Ю.Новикову

_____
(фамилия, имя, отчество обратившегося)

_____

_____
(адрес места жительства)

_____

_____
(сведения о документе, удостоверяющим личность)

_____

_____

Заявление-согласие
субъекта на получение его персональных данных у третьей стороны.

Я, _____, паспорт серии _____, номер _____, выданный _____ _____« ___ » _____ _____ года, в соответствии со ст.86 Трудового Кодекса Российской Федерации _____ на получение моих персональных данных, а именно:
(согласен/не согласен)

_____
_____
_____
_____
_____
(указать состав персональных данных (Ф.И.О, паспортные данные, адрес и т.д.…)
Для обработки в целях _____
_____
_____
(указать цели обработки)
У следующих лиц _____
_____
(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

« ___ » _____ 20_ г.

_____
(подпись)

Приложение № 6
к приказу от 11.01.2021
№01-02/1/2

Главному врачу ГБУЗ ПК «ККСП»
г. Пермь, ул. Братьев Игнатовых, д.4
А.Ю.Новикову

_____
(фамилия, имя, отчество обратившегося)

_____

_____
(адрес места жительства)

_____

_____
(сведения о документе, удостоверяющим личность)

_____

_____

Заявление (согласие) субъекта на передачу его персональных данных третьей стороне.

Я, _____, паспорт серии _____, номер _____, выданный _____ _____« ___ » _____ _____ года, в соответствии со ст.88 Трудового Кодекса Российской Федерации _____ на передачу моих персональных данных, а именно:
(согласен/не согласен)

_____

_____

_____

_____

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

Для обработки в целях _____

_____

_____

(указать цели обработки)

Следующим лицам _____

_____

_____

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

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их передачу.

« ___ » _____ 20_ г.

_____
(подпись)

Приложение № 7
к приказу от 11.01.2021
№01-02/1/2

Журнал учета передачи персональных данных

№	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника
1							
2							
3							
4							

Приложение № 8
к приказу от 11.01.2021
№01-02/1/2

**Журнал учета обращений субъектов персональных данных
о выполнении их законных прав
в области защиты персональных данных**

№	Сведения о запрашивающем лице	Краткое содержание обращения	Цель получения информации	Отметка о предоставлении или отказе в предоставлении информации	Дата передачи/отказа в предоставлении информации	Подпись запрашивающего лица	Подпись ответственного сотрудника
1							
2							
3							
4							

Приложение № 9
к приказу от 11.01.2021
№01-02/1/2

ПЛАН
мероприятий по защите персональных данных в ГБУЗ ПК «ККСП» и его обособленных структурных подразделениях

№ п\п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
1.	Оформление правового основания обработки персональных данных	При вводе информационной системы персональных данных (ИСПДн) в эксплуатацию	Заведующие отделениями, заведующие ОСП	При создании ИСПДн необходимо оформить приказ о вводе ее в эксплуатацию. Приказ оформляется руководителем организации.
2.	Направление в уполномоченный орган (Роскомнадзор) уведомления о своем намерении осуществлять обработку персональных данных с использованием средств автоматизации	При необходимости	Заведующие отделениями, заведующие ОСП	Уведомление направляется при ввводе в эксплуатацию новых информационных систем персональных данных, либо при внесении изменений в существующие
3.	Документальное регламентирование работы с ПД	При необходимости	Заведующие отделениями, заведующие ОСП	Разработка положения по обработке и защите персональных данных, регламента специалиста ответственного за безопасность персональных данных, либо внесение изменений в существующие
4.	Получение письменного согласия субъектов ПД (физических лиц) на обработку ПД в случаях, когда этого требует законодательство	Постоянно	Заведующие отделениями, заведующие ОСП	Письменное согласие получается при передаче ПД субъектами для обработки в ИСПДн, либо для обработки без использования средств автоматизации. Форма согласия приведена в Положении об обработке и защите ПД.
5.	Пересмотр договора с субъектами ПД в части обработки ПД	При необходимости	Заведующие отделениями, заведующие ОСП	(например, в договор может быть включено согласие субъекта на обработку и передачу его ПД). Пересмотр договоров проводится при необходимости и оставляется на усмотрение организации – оператора ПД
6.	Установка сроков обработки ПД и процедуры	При необходимости	Заведующие	Для каждой ИСПДн организацией - оператором ПД должны быть установлены

	их уничтожения по окончании срока обработки		отделениями, заведующие ОСП	сроки обработки ПД, что должно быть документально подтверждено в паспорте на ИСПДн. При пересмотре сроков – необходимые изменения должны быть внесены в паспорт ИСПДн
7.	Ограничение доступа работников к ПД	При необходимости (при создании ИСПДн)	Заведующие отделениями, заведующие ОСП	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона необходимо разграничить доступ к ПД сотрудников организации согласно матрице доступа(сотрудники наделяются минимальными полномочиями доступа, необходимыми для выполнения ими своих обязанностей, например, могут иметь права только на просмотр ПД) Матрица доступа утверждается руководителем организации. При необходимости пересматривается (увольнение, прием новых сотрудников и прочее), подшивается в паспорт ИСПДн
8.	Повышение квалификации сотрудников в области защиты персональных данных	Постоянно	Заведующие отделениями, заведующие ОСП	Ответственных за выполнение работ – не менее раз в два года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за выполнение работ по ИБ)
9.	Инвентаризация информационных ресурсов с целью выявления присутствия и обработки в них ПД	Раз в полгода	Заведующие отделениями, заведующие ОСП	
10.	Классификация информационных систем персональных данных (ИСПД)	При необходимости	Заведующие отделениями, заведующие ОСП	Классификация проводится при создании ИСПДн, при выявлении в информационных системах ПД, при изменении состава, структуры самой ИСПДн или технических особенностей ее построения (изменилось ПО, топология и прочее)
11.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Заведующие отделениями, заведующие ОСП	Разрабатывается при создании системы защиты ИСПДн
12.	Аттестация (сертификация) СЗПД или декларирование соответствия по требованиям безопасности ПД	При необходимости	Заведующие отделениями, заведую	Проводится совместно с лицензиатами ФСТЭК

			щие ОСП	
13.	Эксплуатация ИСПД и контроль безопасности ПД	Постоянно	Заведующие отделениями, заведующие ОСП	

Приложение № 10
к приказу от 11.01.2021
№01-02/1/2

Договор №____
на поручение обработки персональных данных
третьим лицам

г. _____ «____» _____20__г.

Государственное бюджетное учреждение здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника», именуемое в дальнейшем «**Оператор**», в лице _____,
(должность и Ф.И.О)
действующего на основании _____,
с одной стороны, и _____
именуемый в дальнейшем «**Уполномоченная сторона**», в лице _____,
(должность и Ф.И.О)
действующий на основании _____ с другой стороны, вместе именуемые **Стороны,** с соблюдением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», а также другими нормативными правовыми актами Российской Федерации и Пермского края в области защиты персональных данных и безопасности информации, заключили настоящий договор (далее - Договор) о нижеследующем:

1. Термины и определения

1.1. Термины и определения, используемые в настоящем Договоре, применяются в том значении, в котором они установлены в законодательстве Российской Федерации о персональных данных.

2. Предмет договора

2.1. Уполномоченная сторона обязуется по заданию Оператора оказывать услуги в виде обработки персональных данных (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение) в соответствии с перечнем, приведенным в п.5 настоящего Договора

2.2. Уполномоченная сторона обязуется принять меры к обеспечению конфиденциальности и безопасности персональных данных представляемых ей Оператором для обработки, и выполнять иные обязательства в соответствии с настоящим Договором.

3. Обязанности, связанные с безопасностью

3.1 Уполномоченная сторона обязана совершать какие-либо действия в отношении

персональных данных, которые она обрабатывает от имени Оператора, исключительно в соответствии с указаниями Оператора.

3.2 Уполномоченная сторона обязана принимать надлежащие технические и организационные меры по обеспечению безопасности в соответствии с требованиями законодательства в части защиты персональных данных.

3.3 В случае реорганизации или ликвидации одной из Сторон, Уполномоченная Сторона обязуется незамедлительно уничтожить или, по просьбе Оператора, вернуть все полученные Уполномоченной Стороной персональные данные.

4. Конфиденциальность

4.1. Уполномоченная сторона соглашается с тем, что она обязана обрабатывать персональные данные от имени Оператора, соблюдая конфиденциальность обработки. В частности, если Уполномоченная сторона не получила письменного согласия от Оператора, она не будет раскрывать персональные данные, переданные ей Оператором/для Оператора/от имени Оператора посторонним лицам.

4.2. Если Уполномоченная сторона обязана в силу закона раскрыть персональные данные третьей стороне, она раскрывает эту информацию только этой стороне и только в той степени, насколько этого требует закон.

4.3. Если произойдут события или действия, в результате которых Уполномоченная сторона будет вынуждена разгласить персональные данные, она немедленно оповещает Оператора, субъекта персональных данных в случае получения запроса, уполномоченный орган по защите прав субъектов персональных данных об этих событиях или действиях в письменной форме, и предпринимает все возможные действия, чтобы избежать дальнейшего разглашения персональных данных.

4.4. Уполномоченная сторона не вправе использовать персональные данные, переданные ей Оператором, иначе, чем соответствующие полномочия определены настоящим договором, и с соблюдением требований, установленных федеральным законом к обработке и защите персональных данных.

4.5. Требования сохранять конфиденциальность информации распространяются на весь срок действия Договора и сохраняют свою силу в течение _____ лет с момента прекращения действия Договора.

4.6. Вышеуказанные обязательства конфиденциальности не распространяются на обезличенную и общедоступную информацию.

4.7. Никакие положения настоящего Договора не освобождают Стороны от соблюдения правовых требований, предъявляемых уполномоченным органом по защите прав субъектов персональных данных или судом. Стороны должны, по мере возможности обсуждать друг с другом ответы на запросы на получение информации со стороны уполномоченного органа по защите прав субъектов персональных данных или судов.

5. Перечень персональных данных для обработки

5.1. Перечень персональных данных Оператора, обрабатываемых Уполномоченной стороной, включает в себя (указать): персональные данные первой, второй и третьей категории.

6. Обязательства Сторон

6.1. Оператор обязуется:

6.1.1. Предоставить Уполномоченной стороне все необходимые для обработки данные, определить цель их обработки и перечень действий над ними.

6.1.2. Предоставить Уполномоченной стороне достоверные персональные данные и сообщать обо всех изменениях в составе персональных данных, переданных для обработки.

6.1.3. Сообщить субъекту персональных данных или его законному представителю о заключении настоящего Договора и передаче Уполномоченной стороне его персональных данных для обработки.

6.1.4. Требовать от Уполномоченной стороны представления надлежащим образом оформленной отчетной документации и материалов, подтверждающих исполнение обязательств по настоящему Договору.

6.1.5. Своевременно принять и оплатить надлежащим образом оказанные услуги в соответствии с настоящим Договором.

6.1.6. Направлять Уполномоченной стороне уведомления об уплате в добровольном порядке сумм неустойки (пеней, штрафов), предусмотренных настоящим Договором за неисполнение (ненадлежащее исполнение) Уполномоченной стороной своих обязательств по настоящему Договору.

6.1.7.. В случае неуплаты Уполномоченной стороной в добровольном порядке предусмотренных настоящим Договором сумм неустойки (пеней, штрафов) взыскивать их в судебном порядке.

6.2. Уполномоченная сторона обязуется:

6.2.1. Обрабатывать полученные персональные данные в соответствии с законодательством и иными нормативными правовыми актами Российской Федерации и Пермского края.

6.2.2. При обработке персональных данных обеспечить необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

6.2.3. Обеспечивать конфиденциальность обрабатываемых персональных данных, а также применять меры по их защите, в соответствии с категорией и объемом обрабатываемых персональных данных.

6.2.4. Не разглашать полученные от Оператора персональные данные никому, кроме следующих лиц:

- сотрудников и субподрядчиков принадлежащих к Сторонам Договора, которые напрямую связаны с обработкой Уполномоченной стороне персональных данных;
- субъектов персональных данных или их законных представителей, которые хотят получать информацию, касающуюся своих персональных данных;
- уполномоченным органам по защите прав субъектов персональных данных.

6.2.5. Следить за тем, чтобы ее сотрудники и субподрядчики соблюдали условия конфиденциальности и требования по защите персональных данных.

6.2.6. Проследить, чтобы любая третья сторона, которой были раскрыты персональные данные, соблюдала условия конфиденциальности.

6.2.7. По письменному требованию Оператора подтвердить в письменной форме, что она соблюдает обязательства по настоящему Договору в части обработки и защиты персональных данных.

6.2.8. Требовать своевременного подписания Оператором актов приемки выполненных работ по настоящему Договору.

6.2.9. Требовать своевременной оплаты оказанных услуг.

6.2.10. Исполнять иные обязательства, предусмотренные действующим законодательством и Договором.

7. Ответственность Сторон

7.1. За неисполнение или ненадлежащее исполнение своих обязательств, установленных настоящим Договором, Оператор несет ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. В случае просрочки исполнения Оператором обязательств по оплате Цены Договора Уполномоченная сторона вправе потребовать от Оператора уплату неустойки. Неустойка начисляется за каждый день просрочки исполнения обязательства по оплате *Цены Договора* начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства по оплате Цены Договора. Размер такой неустойки устанавливается в размере одной трехсотой действующей на день уплаты неустойки ставки рефинансирования Центрального банка Российской Федерации от Цены Договора. Оператор освобождается от уплаты неустойки, если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине Уполномоченной стороны.

7.3 Уполномоченная сторона несет ответственность в соответствии с действующим законодательством РФ:

- за ненадлежащее проведение операций с персональными данными переданными ему Оператором;
- за разглашение персональных данных;
- за действия, которые осуществляют сотрудники и субподрядчики с персональными данными Оператора, повлекшие нарушения законодательства в области обработки и защиты персональных данных и (или) права субъектов персональных данных.

7.4. Уполномоченная сторона не несет ответственность за невыполнение условий настоящего Договора, в случае возникновения обстоятельств непреодолимой силы (форс-мажорных), повлекших за собой неисполнение Уполномоченной стороной обязательств по настоящему Договору.

7.5. В случае просрочки исполнения Уполномоченной стороной обязательств, предусмотренных настоящим Договором, Оператор вправе потребовать уплату неустойки (штрафа, пеней). Неустойка (штраф, пени) начисляется за каждый день просрочки исполнения обязательства, предусмотренных Договором, начиная со дня, следующего после дня истечения установленного настоящим договором срока исполнения обязательства. Размер такой неустойки (штрафа, пеней) устанавливается Договором в размере не менее одной трехсотой действующей на день уплаты неустойки (штрафа, пеней) ставки рефинансирования Центрального банка Российской Федерации. Уполномоченная сторона освобождается от уплаты

неустойки (штрафа, пеней), если докажет, что просрочка исполнения указанного обязательства произошла вследствие непреодолимой силы или по вине Оператора.

8. Порядок расчетов

8.1. Оператор оплачивает Уполномоченной стороне услуги, предоставляемые, по настоящему Договору из расчета в месяц _____ руб. (сумма прописью) с учетом НДС.

8.2. Цена Договора составляет _____ руб. (сумма прописью) в т.ч. НДС 18%.

8.3. Оплата по Договору производится ежемесячно, путём перечисления денежных средств в российских рублях на расчётный счёт Уполномоченной стороны в следующем порядке: в течение 5 банковских дней со дня подписания Оператором актов приемки выполненных работ за фактически оказанные в предыдущем месяце услуги на основании счета и счета-фактуры.

8.4. Цена Договора включает в себя все затраты, издержки и иные расходы Уполномоченной стороны, в том числе сопутствующие, связанные с исполнением настоящего Договора.

8.5. Обязательства Оператора по оплате Цены Договора считаются исполненными с момента списания денежных средств в размере, составляющем Цены Договора, с банковского счета Оператора, указанного в статье 13 настоящего Договора.

8.6. В случае изменения расчетного счета Уполномоченной стороны последний обязан в трехдневный срок в письменной форме сообщить об этом Оператору с указанием новых реквизитов расчетного счета.

В противном случае все риски, связанные с перечислением Оператором денежных средств на указанный в настоящем Договоре счет Уполномоченного лица, несет Уполномоченное лицо.

9. Порядок разрешения споров

9.1. Все споры и разногласия, возникшие в связи с исполнением настоящего Договора, его изменением, расторжением или признанием недействительным, Стороны будут стремиться решить путем переговоров, а достигнутые договоренности оформлять в виде дополнительных соглашений, подписанных Сторонами и скрепленных печатями.

9.2. В случае невозможности разрешения споров путем переговоров стороны передают их на рассмотрение в Арбитражный суд Пермского края.

Статья 10. Обстоятельства непреодолимой силы

10.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору в случае, если оно явилось следствием действия обстоятельств непреодолимой силы, а именно чрезвычайных и непредотвратимых при данных условиях обстоятельств: стихийных природных явлений (землетрясений, наводнений, пожара и т.д.), действий объективных внешних факторов (военные действия, акты органов государственной власти и управления и т.п.), а также других чрезвычайных обстоятельств, подтвержденных в установленном

законодательством порядке, препятствующих надлежащему исполнению обязательств по настоящему Договору, которые возникли после заключения настоящего Договора, на время действия этих обстоятельств, если эти обстоятельства непосредственно повлияли на исполнение Сторонами своих обязательств, а также которые Стороны были не в состоянии предвидеть и предотвратить.

10.2. Если в результате обстоятельств непреодолимой силы оказываемым услугам нанесен значительный, по мнению одной из Сторон, ущерб, то эта Сторона обязана уведомить об этом другую Сторону в 3-дневный срок, после чего Стороны обязаны обсудить целесообразность дальнейшего оказания услуг и заключить дополнительное соглашение с обязательным указанием новых объемов, сроков и стоимости работ, которое с момента его подписания становится неотъемлемой частью Договора, либо расторгнуть настоящий Договор. Если обстоятельства, указанные в п. 10.1, будут длиться более 2 (двух) календарных месяцев с даты соответствующего уведомления, каждая из Сторон вправе расторгнуть настоящий Договор без требования возмещения убытков, понесенных в связи с наступлением таких обстоятельств.

10.3. Если, по мнению Сторон, оказание услуг может быть продолжено в порядке, действовавшем согласно настоящему Договору до начала действия обстоятельств непреодолимой силы, то срок исполнения обязательств по Договору продлевается соразмерно времени, в течение которого действовали обстоятельства непреодолимой силы и их последствия.

11. Срок действия и порядок изменения, расторжения Договора

11.1. Договора вступает в силу со дня его подписания Сторонами и действует до "__" _____ 20___ г.

11.2. Изменение и дополнение настоящего Договора возможно по соглашению Сторон. Все изменения и дополнения оформляются в письменном виде путем подписания Сторонами дополнительных соглашений к Договору. Дополнительные соглашения к Договору являются его неотъемлемой частью и вступают в силу с момента их подписания Сторонами.

11.2. Настоящий Договор может быть расторгнут:

- по соглашению Сторон, совершенному в письменной форме за подписью уполномоченных лиц сторон;
- в судебном порядке, при существенном нарушении условий Договора Уполномоченной стороной.

11.2. Сторона, которой направлено предложение о расторжении Договора по соглашению сторон, должна дать письменный ответ по существу в срок не позднее 5 (пяти) календарных дней с даты его получения

12. Прочие условия

12.1. Все уведомления Сторон, связанные с исполнением настоящего Договора, направляются в письменной форме по почте заказным письмом по фактическому адресу Стороны, указанному в статье 13 настоящего Договора, или с использованием факсимильной связи, электронной почты с последующим представлением оригинала. В случае направления уведомлений с использованием почты уведомления считаются полученными Стороной в день фактического получения, подтвержденного отметкой почты. В случае отправления уведомлений посредством факсимильной связи и

электронной почты уведомления считаются полученными Стороной в день их отправки.

12.2. Договор составлен в 2 (двух) экземплярах, по одному для каждой из Сторон, имеющих одинаковую юридическую силу.

12.3. Во всем, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.

13. Адреса, реквизиты и подписи Сторон

Оператор:	Уполномоченная сторона:
Адреса:	Адреса:
- юридический:	- юридический:
- фактический:	- фактический:
Телефон _____, факс _____	Телефон _____, факс _____
Электронный адрес:	Электронный адрес:
Получатель: л/с _____	Получатель: л/с _____
ОГРН _____	ОГРН _____
ИНН _____	ИНН _____
КПП _____	КПП _____
БИК _____	БИК _____
р/с _____	р/с _____
_____	_____
(должность подписывающего и его Ф.И.О)	(должность подписывающего и его Ф.И.О)
М.П.	М.П.

Соглашение №_____о конфиденциальности

г. _____ «____» _____201__г.

Настоящее Соглашение заключено между Государственным бюджетным учреждением здравоохранения Пермского края «Краевая клиническая стоматологическая поликлиника» (далее «Передающая Сторона»), в лице _____
действующего на основании Устава, с одной стороны, и _____
_____ (далее «Получающая Сторона»), в лице _____, действующего на основании Устава, далее совместно именуемыми «Стороны», а каждый в отдельности «Сторона», договорились о нижеследующем:

1. Для целей настоящего Соглашения термин «Конфиденциальная Информация» означает любую информацию Передающей Стороны, а равно сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе персональные данные субъектов, переданную Получающей Стороне и обозначенную как конфиденциальная.

Информация не является конфиденциальной в случае, если такая информация:

(а) является или становится общеизвестной не в результате нарушения настоящего Соглашения;

(б) находилась в распоряжении Получающей Стороны до ее получения от Передающей Стороны;

(в) получена Получающей Стороной от третьих лиц, в отношении которых у Получающей Стороны не было сведений о неправомерном раскрытии такими лицами данной информации.

Термин «персональные данные» означает любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Конфиденциальная информация не может без предварительного письменного разрешения Передающей Стороны копироваться или иным образом воспроизводиться Получающей Стороной.

2. Передача Передающей Стороной Конфиденциальной Информации Получающей Стороне может осуществляться письменно, устно или путем передачи (предоставления) конфиденциальной информации на магнитных носителях, мультимедийными средствами или в виде фотографий или другими способами.

Передача Конфиденциальной Информации по настоящему Соглашению оформляется двусторонним актом, подписываемым представителями Сторон, с указанием количества информации, ее носителя, объема, формата и других идентификационных признаков.

В случае передачи Конфиденциальной Информации устно или визуально на переговорах либо совещаниях между Сторонами настоящего Соглашения, ее

передача фиксируется путем подписания представителями Сторон соответствующего протокола, с указанием характера Конфиденциальной Информации, ее объема, формата и других идентификационных признаков.

3. Настоящее Соглашение не предоставляет Получающей Стороне никаких прав в отношении Конфиденциальной Информации кроме права использования, необходимого для целей

_____

(указать в каких целях будет использоваться передаваемая информации)

4. В отношении Конфиденциальной Информации Получающая Сторона обязуется:

4.1. Не использовать Конфиденциальную Информацию в каких-либо других целях, кроме как для целей, определенных в пункте 3 Соглашения;

4.2. Принимать меры по охране Конфиденциальной Информации, находящейся на хранении или используемой ею, с такой же степенью, с какой она охраняет собственную конфиденциальную информацию;

4.3. Раскрывать полученную Конфиденциальную Информацию своим сотрудникам, которым требуется получение такой Конфиденциальной Информации только в тех пределах, которые необходимы для целей, определенных в пункте 3 Соглашения, соответственно проинформировав их о конфиденциальном характере информации и ограничениях, связанных с ее использованием, а равно иным способом обеспечив соблюдение конфиденциальности информации;

4.4. Раскрывать полученную Конфиденциальную Информацию третьим лицам только при условии получения предварительного письменного согласия Передающей Стороны на такое раскрытие. При этом Передающая Сторона вправе заключить с одобренными ею третьими лицами отдельные соглашения о конфиденциальности в отношении Конфиденциальной Информации;

4.5. По требованию Передающей Стороны возвратить ей или уничтожить Конфиденциальную Информацию, которая была получена Получающей Стороной в течение срока действия настоящего Соглашения и находится у Получающей Стороны на момент получения соответствующего требования Передающей Стороны.

5. Получающая Сторона имеет право без предварительного письменного согласия Передающей Стороны предоставлять Конфиденциальную Информацию тем лицам, раскрытие информации в пользу которых предусмотрено требованиями действующего законодательства, включая любое предписание уполномоченного государственного или судебного органа и только в порядке, установленном таким документом. В случае раскрытия Конфиденциальной информации на основании настоящего пункта Получающая сторона ограничит передачу информации запрашиваемым объемом и проинформирует Передающую сторону о факте получения запроса о предоставлении информации в максимально короткие сроки.

6. После окончания действия настоящего Соглашения либо в случае реорганизации или ликвидации Получающей Стороны, Получающая Сторона обязуется незамедлительно уничтожить или, по просьбе Передающей Стороны, вернуть всю полученную Конфиденциальную Информацию и копии, сделанные с нее.

7. Все споры и разногласия, возникающие в связи с исполнением настоящего Соглашения, Стороны будут разрешать путем переговоров, а достигнутые

договоренности оформлять в виде дополнительных соглашений, подписанных Сторонами и скрепленных печатями. В случае невозможности разрешения споров путем переговоров стороны передают их на рассмотрение в Арбитражный суд Пермского края.

8. В случае нарушения Получающей Стороной положений настоящего Соглашения, Получающая Сторона компенсирует все убытки Передающей Стороны, вызванные таким нарушением.

9. В случае признания недействительным или невозможным исполнение любого положения настоящего Соглашения полностью или частично по любой причине остальные положения настоящего Соглашения сохраняют юридическую силу и действие в полном объеме настолько, насколько это позволяет действующее законодательство.

10. Все изменения и дополнения к настоящему Соглашению действительны лишь в случае, если они совершены в письменной форме и подписаны надлежаще уполномоченными представителями Сторон.

11. Настоящее Соглашение вступает в силу с даты его подписания, действует по «____» _____ 20___ года.

12. Настоящее соглашение может быть расторгнуто по договоренности Сторон либо по инициативе одной из Сторон с предупреждением в письменной форме другой Стороны не менее чем за 30 календарных дней до расторжения настоящего соглашения.

13. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

14. Адреса, реквизиты и подписи Сторон

Передающей Стороны:	Получающая Сторона:
Адреса:	Адреса:
- юридический:	- юридический:
- фактический:	- фактический:
Телефон _____, факс _____	Телефон _____, факс _____
Электронный адрес:	Электронный адрес:
ОГРН _____	ОГРН _____
ИНН _____	ИНН _____
КПП _____	КПП _____
_____	_____
(должность подписывающего и его Ф.И.О)	(должность подписывающего и его Ф.И.О)
М.П.	М.П.