Утверждаю

Генеральный директор ООО «Никор-Н»

_____Коробкова Н. А.

01 июня 2017 года

Политика Общества с ограниченной ответственностью «Никор-Н» 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 N 152-ФЗ «О персональных данных» (далее — Закон о ПДн) и является основополагающим внутренним регулятивным документом Общества с ограниченной ответственностью «Никор-Н» (далее — Общество), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее — ПДн), оператором которых является Общество.

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 Обществе, 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 Обществом 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 Обществом участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Общество становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Общества 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 Обществом.

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

2.1. Обработка ПДн в Обществе осуществляется в связи с осуществлением профессиональной деятельности Общества в соответствии:

1) Федеральным законом от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

2) Федеральным законом от 29.11.2010 N 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации

Кроме того, обработка ПДн в Обществе осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Общество выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Обществом своих прав и обязанностей как юридического лица, а также при взаимодействии с органами государственной власти в сфере лицензирования медицинской деятельности, органами государственной власти г. Москвы при реализации совместных программ и проектов, Пенсионного Фонда, Фонда Социального Страхования, Фонда обязательного медицинского страхования, Центра квотирования рабочих мест и другими органами власти и местного самоуправления.

2.2. В рамках осуществления медицинской деятельности обрабатываются Обществом ПДн:

Пациентов, а также иных лиц, обратившихся за оказанием медицинской помощи.

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

2.4. В связи с реализацией своих прав и обязанностей, Обществом обрабатываются ПДн физических лиц, являющихся контрагентами Общества по гражданско-правовым договорам, физических лиц, ПДн которых используются для осуществления пропускного режима в занимаемых Обществом помещениях, а также граждан, письменно обращающихся в Общество по вопросам его деятельности (помимо лиц, указанных в пунктах 2.2 — 2.3 Политики).

2.5. В рамках взаимодействия с учредителями Общества ПДн обрабатываются в ходе формирования органов управления Общества.

2.6. Специальные категории персональных данных:

В рамках основной уставной деятельности Общество обрабатывает ПДн о состоянии здоровья обратившихся в Общество пациентов.

Обработка данных о состоянии здоровья производится при наличии одного из приведенных ниже условий:

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

2) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

3) 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;

4) обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования (обязательного медицинского страхования), в соответствии со страховым законодательством.

2.7. Обработка биометрических данных:

1) Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, обрабатываются только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящего пункта.

2) Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию. При наличии указанных оснований по запросу компетентных органов Общество может предоставлять биометрические данные о пациентах, проводить их сравнение и давать заключение об идентификации.

2.8. ПДн получаются и обрабатываются Обществом на основании федеральных законов, а в необходимых случаях — при наличии письменного согласия субъекта ПДн.

2.9. В целях исполнения возложенных на Общество функций Общество в установленном порядке вправе поручить обработку ПДн третьим лицам.

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

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

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

2.12. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости — и актуальность по отношению к целям обработки. Общество 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 Обществе является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Общество 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 Обществе осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Общества (далее — ИС) и других имеющихся в Обществе 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) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации

угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

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

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

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

10) открытость алгоритмов и механизмов защиты: структура, технологии и алгоритмы функционирования системы защиты ПДн Общества (далее — СЗПДн) не дают возможности преодоления имеющихся в Обществе систем защиты возможными нарушителями безопасности ПДн;

11) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

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

13) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Общества предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Общества до заключения договоров;

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

15) 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 обществе ПДн имеют лица, уполномоченные приказом Общества, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой определенной законодательством функции Общества закрепляются за соответствующими работниками Общества.

4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Общества. Допуск Работников к обработке ПДн осуществляется согласно внутренних локальных актов Общества. Соответствующие полномочия (роль пользователя) вносятся в должностные обязанности Работников.

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

4.4. Факты получения доступа к ИСПДн, а также факты обработки ПДн регистрируются, в том числе с использованием средств обеспечения информационной безопасности. Информация о фактах обработки ПДн хранится в Обществе, включая ИС, в течение трех лет.

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

5. Реализация Политики

5.1. Общество 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. Ответственность за организацию обработки ПДн в Обществе несет один из заместителей Генерального директора Общества или иной работник, определяемый Генеральным директором Общества.

Ответственный за организацию обработки ПДн в Обществе, в частности, обязан:

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

2) доводить до сведения Работников положения нормативных правовых актов и внутренних регулятивных документов Общества 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. Общество осуществляет обработку ПДн без использования средств автоматизации, а также с использованием таких средств.

5.4. При обработке ПДн без использования средств автоматизации Общество, 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) охранность материальных носителей ПДн;

5) условия хранения, исключающие несанкционированный доступ к ПДн, а также смешение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

6) 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 Обществе могут создаваться ИСПДн.

Все ИСПДн, в случае их создания, 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 Обществе с использованием средств автоматизации ведется только в ИСПДн. В Обществе 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 Обществе создается СЗПДн (Система защиты персональных данных).

Объектами защиты СЗПДн являются информация, обрабатываемая Обществом 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 Общества по вопросам обработки и защиты ПДн, контроль за исполнением в Обществе требований нормативных правовых актов и внутренних регулятивных документов Общества 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 (при необходимости) Общества и должностных обязанностях Работников требований по соблюдению установленного порядка обработки и защиты ПДн;

5) разработку и введение в действие внутренних регулятивных документов Общества 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 Общества 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 Общества, так и при взаимодействии с контрагентами Общества, 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) организацию технического оснащения объектов и ИСПДн в соответствии с существующими требованиями к информационной безопасности;

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

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

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

15) организацию необходимых мероприятий с Работниками, а также собеседование с лицами, претендующими на работу в Обществе, изучение их биографии и проверку предоставляемых сведений; обучение Работников требованиям информационной безопасности;

16) осуществление контроля эффективности организационных мер защиты;

17) разработку защитных технических решений:

а) при стратегическом планировании архитектуры ИС;

б) выборе технических средств обработки информации;

в) разработке и (или) приобретении программного обеспечения;

18) 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 Обществе 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 добывания, 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 в помещения, где размещены технические средства, позволяющие осуществлять обработку ПДн, а также хранятся носители информации, содержащие 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 Обществе может быть создано структурное подразделение либо назначен ответственный работник, либо заключен договор с третьим лицом, наделенном полномочиями для работы ИСПДн, 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 Общества 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 Обществе 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 Обществе проводятся периодические проверки условий обработки ПДн. Такие проверки осуществляются ответственным за организацию обработки ПДн в Обществе либо комиссией, образуемой Генеральным директором Общества.

О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывается Генеральному директору Общества.