Политика ООО «Клиника неврологии» в отношении обработки и защиты персональных данных

Утверждена
решением № 2 единоличного исполнительного органа
от 27.06.2015 г.

ПОЛИТИКА
ООО «Клиника неврологии»
в отношении обработки и защиты персональных данных

Общие положения

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 ООО «Клиника неврологи» (далее – Общество), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Общество.
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.
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.
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.
5. Обработка ПДн в Обществе осуществляется в связи с оказанием медицинской помощи и осуществлении медицинской деятельности согласно лицензии на осуществление медицинской деятельности № ЛО 59-01-003660 от 27 мая 2016 года и ФЗ «Об основах охраны здоровья граждан в Российской Федерации».
6. 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.
7. В рамках осуществления медицинской деятельности Общества ПДн обрабатываются:

- в ходе записи на прием к врачу, а также вызова врача на дом, в том числе с использованием Интернет-сайта клиники;
- в ходе проведения приема врачом и заполнения им амбулаторной карты пациента;
- в ходе хранения амбулаторных карт пациентов;

При этом обрабатываются ПДн пациентов и/или их законных представителей.

8. 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.

9. В связи с реализацией своих прав и обязанностей как юридического лица Обществом обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) Общества по гражданско-правовым договорам, и представителей юридических лиц, ПДн иных физических лиц, письменно обращающихся в Общество по вопросам его деятельности.

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

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 ПДн уничтожаются или обезличиваются по истечении сроков, установленных законом.

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.

Принципы обеспечения безопасности персональных данных

13. 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.

14. Для обеспечения безопасности ПДн Общество руководствуется следующими принципами:

- законность: защита ПДн основывается на положениях нормативных правовых актов и законодательства Российской Федерации;
- 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;
- 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;
- непрерывность: защита ПЛн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Обществе с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

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

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

- 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;

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

Доступ к обрабатываемым персональным данным

15. Доступ к обрабатываемым в Обществе ПДн имеют лица, уполномоченные приказом Общества, а также лица, чьи ПДн подлежат обработке.

16. Доступ Работников к обрабатываемым ПДн осуществляются в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Общества.

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

18. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Обществом, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Общества.

Реализуемые требования к защите персональных данных

19. Общество принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствие с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

20. Состав указанных в п.19 Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) Обществом исходя из требований:

- Закона о ПДн;

- главы 14 Трудового кодекса Российской Федерации;

- Федерального закона от 21.111.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн»;

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

- иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

21. В предусмотренных законодательством случаях обработка ПДн осуществляется Обществом с согласия субъектов ПДн.

22. Обществом производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

23. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

24. Обществом осуществляется ознакомление работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.

25. При обработке ПДн с использованием средств автоматизации Обществом, в частности, применяются следующие меры:

- назначается Ответственный за организацию обработки ПДн и определяется его компетенция;

- утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

- осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивными документам Общества;

- проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

26. Обеспечение безопасности ПДн в Обществе при их обработке достигается, в частности, путем:

- определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

- определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Обществом могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки СЗПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

- применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

27. В Обществе, в том числе, осуществляются:

- оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

- учет машинных носителей ПДн, обеспечение их сохранности;

- обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

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

- установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение защиты ПДн в Обществе при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

● обособления ПДн от иной информации;

● недопущение фиксации на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы;

● использование отдельных материальных носителей для обработки каждой категории ПДн;

● принятие мер по обеспечению раздельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

● соблюдения требований:

- к раздельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

- уточнению ПДн;

- уничтожению или обезличиванию части ПДн;

- использованию типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн.

Сведения, составляющие врачебную тайну

28. Врачебной тайной являются сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении.

29. Обществом не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека.

30. С письменного согласия гражданина или его законного представителя Общество имеет право разглашения сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях.

31. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

- в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю. С учетом положений пункта 1 части 9 статьи 20 Федерального закона от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

- в целях осуществления уполномоченными федеральными органами исполнительной власти контроля за исполнением лицами, признанными больными наркоманий либо потребляющими наркотические средства или психотропные вещества без назначения врача либо новые потенциально опасные психоактивные вещества, возложенной на них при назначении административного наказания судом обязанности пройти лечение от наркомании, диагностику, профилактические мероприятия и (или) медицинскую реабилитацию;

- в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», для информирования одного из его родителей или иного законного представителя;

- в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

-в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

- в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность, и в соответствии с частью 6 статьи 43.1 Федерального закона от 4 декабря 2007 года № 329 «О физической культуре и спорте в Российской Федерации» несчастного случая с лицом, проходящим спортивную подготовку и не состоящим в трудовых отношениях с физкультурно-спортивной организацией, не осуществляющей спортивной подготовки и являющейся заказчиком услуг по спортивной подготовке, во время прохождения таким лицом спортивной подготовки в организации, осуществляющей спортивную подготовку, в том числе во время его участия в спортивных соревнованиях, предусмотренных реализуемыми программами спортивной подготовки;

- при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

- в целях осуществления учета и контроля в системе обязательного социального страхования;

- в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».