УТВЕРЖДЕНО
приказом ФГАУ «НМИЦ здоровья детей» Минздрава России
от 22.11.2021 № 18-132/АХ

ПОЛИТИКА
обработки и защиты персональных данных ФГАУ «НМИЦ здоровья детей» Минздрава России

1. Общие положения

1.1. Политика обработки и защиты персональных данных в федеральном государственном автономном учреждением «Национальный медицинский исследовательский центр здоровья детей» Минздрава России» (далее – Политика) разработана в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ), постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также иных нормативных правовых актов Российской Федерации, регулирующих вопросы обработки персональных данных.

Политика является нормативным актом федерального государственного автономного учреждения «Национальный медицинский исследовательский центр здоровья детей» Министерства здравоохранения Российской Федерации (далее – Учреждение), определяющим основные принципы и ключевые направления деятельности Учреждения в области обработки и защиты персональных данных.

1.2. Политика разработана в целях реализации требований законодательства Российской Федерации в области обработки и защиты персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн, а также установления ответственности работников Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Политика распространяется на отношения по обработке и защите персональных данных, полученных Учреждением как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера Политика не может быть распространена на отношения по обработке и защите персональных данных, полученных до ее утверждения.

1.4. Учреждение, как оператор персональных данных самостоятельно либо совместно с другими лицами организует и (или) осуществляет обработку персональных данных, а также определяет цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.5. Действующая редакция Политики хранится в месте нахождения Учреждения по адресу: город Москва, Ломоносовский проспект, д. 2, корп. 1, неограниченный доступ к электронной версии Политики осуществляется путем размещения на сайте Учреждения по адресу: www. nczd.ru.

2. Термины и принятые сокращения

2.1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу – субъекту персональных данных.

2.2. 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.

2.3. Оператор персональных данных – юридическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

2.4. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.5. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.6. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.7. 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.

2.8. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.9. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.10. Информационная система персональных данных (ИСПД) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.11. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.12. Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

2.13. Представитель субъекта персональных данных (далее по тексту «представитель») – законный представитель несовершеннолетнего лица – родитель,

усыновитель, опекун, попечитель, приемный родитель, орган опеки и попечительства, а также иной представитель, действующий в соответствии с законодательством Российской Федерации.

2.14. Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

2.15. Врачебная тайна – сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, когда с письменного согласия гражданина или его законного представителя сведения, составляющие врачебную тайну, могут быть переданы 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. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается только в случаях, предусмотренных законодательством Российской Федерации.

3. Категории субъектов персональных данных

3.1. Учреждение обрабатывает персональные данные следующих категорий субъектов персональных данных:

– персональные данные работников Учреждения в связи с трудовыми отношениями и касающиеся конкретного работника Учреждения;

– персональные данные детей работников Учреждения в связи с оформлением льгот в соответствии с требованиями законодательства Российской Федерации;

– персональные данные физических лиц, являющихся близкими родственниками работников Учреждения;

– персональные данные физических лиц, уволившихся из Учреждения, в объеме, необходимом для соблюдений требования законодательства Российской Федерации;

– персональные данные физических лиц в связи с гражданско-правовыми отношениями с Учреждением;

– персональные данные пациентов Учреждения;

– персональные данные законных представителей пациентов Учреждения;

– персональные данные работников юридических лиц, являющихся контрагентами Учреждения, необходимые для выполнения своих обязательств в рамках договорных отношений с контрагентом и для выполнения требований законодательства Российской Федерации;

– персональные данные посетителей в связи с контрольно-пропускным режимом.

3.2. Перечень обрабатываемых персональных данных содержится в приложении №1 к Политике.

4. Цели обработки персональных данных

4.1. Учреждение осуществляет обработку персональных данных в следующих целях:

– осуществления медицинской деятельности, предусмотренной законодательством Российской Федерации, в соответствии с имеющимися лицензиями и Уставом Учреждения;

– защиты жизни, здоровья или иных интересов субъектов персональных данных;

– заключения, исполнения, прекращения трудовых, гражданско-правовых договоров с физическими, юридическими лицами, индивидуальными предпринимателями и иными лицами в случаях, предусмотренных законодательством Российской Федерации;

– организации кадрового делопроизводства и учета в соответствии с законодательством Российской Федерации;

– обеспечения соблюдения законов и иных нормативно-правовых актов Российской Федерации, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам;

– исполнения требований налогового законодательства Российской Федерации в связи с исчислением и уплатой налога на доходы физических лиц, а также иных обязательных выплат;

– исполнения требований пенсионного законодательства Российской Федерации при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, иными законодательными актами Российской Федерации;

– обеспечения контрольно-пропускного и внутриобъектового режимов на объектах Учреждения;

– исполнение судебных актов, актов других органов, подлежащих исполнению в соответствии с законодательством Российской Федерации.

5. Сроки обработки персональных данных

5.1. Сроки обработки персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, а также иными требованиями законодательства Российской Федерации и нормативными актами Учреждения.

5.2. В Учреждении создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в Учреждения персональных данных, содержащихся в документах, установлены постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Принципы обеспечения безопасности персональных данных

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

6.2. Для обеспечения безопасности персональных данных Учреждение руководствуется следующими принципами:

– законность и достаточность: защита персональных данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты персональных данных и осуществляется только в соответствии с объемом, характером и целями обработки персональных данных, заранее определенных и заявленных при сборе персональных данных, а также в соответствии с полномочиями Учреждения, как оператора персональных данных. Не допускается сбор и обработка персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– достоверность: содержание персональных данных отражает достоверную информацию, а также их достаточность для целей обработки, заявленных при сборе персональных данных;

– системность: обработка персональных данных в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных. Не допустимо объединять базы, содержащие персональных данных, созданные для несовместимых между собой целей;

– комплексность: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения и других имеющихся в Учреждении систем и средств защиты;

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

– своевременность: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки. Хранения персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки. Уничтожение персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении таких целей;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты персональных данных осуществляется на основании результатов анализа практики обработки персональных данных в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности персональных данных, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности персональных данных возлагается на работников Учреждения в пределах их обязанностей, связанных с обработкой и защитой персональных данных;

– минимизация прав доступа: доступ к персональным данным предоставляется работникам Учреждения только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты персональных данных при изменении характеристик функционирования информационных систем персональных данных Учреждения, а также объема и состава обрабатываемых персональных данных;

– специализация и профессионализм: реализация мер по обеспечению безопасности персональных данных осуществляются работниками Учреждения, имеющими необходимые для этого квалификацию и опыт;

– эффективность процедур отбора кадров: кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию работников Учреждения, позволяющую исключить или минимизировать возможность нарушения ими безопасности персональных данных;

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

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты персональных данных, а результаты контроля регулярно анализируются.

6.3. В Учреждении не производится обработка персональных данных, несовместимая с целями их сбора. Если иное не предусмотрено законодательством Российской Федерации, по окончании обработки персональных данных, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, персональные данные уничтожаются или обезличиваются.

6.4. При обработке персональных данных обеспечиваются их точность, достаточность, а при необходимости – актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных персональных данных.

7. Обработка персональных данных.

7.1. Все персональные данные должны быть получены от самого субъекта персональных данных или действующего от его имени представителя. Если персональные данные субъекта персональных данных можно получить только у третьей стороны, то субъект персональных данных или его представитель должны быть уведомлены об этом и от них должно быть получено согласие.

7.2. Учреждение сообщает субъекту персональных данных или его законному представителю о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных, перечне действий с персональных данных, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта персональных данных или его представителя дать письменное согласие на их получение.

7.3. Документы, содержащие персональных данных создаются путем:

– копирования оригиналов документов (паспорт, документ об образовании, пенсионное свидетельство и др.);

– внесения сведений в учетные формы;

– получения оригиналов необходимых документов (трудовая книжка, медицинская книжка, медицинское заключение, и иные документы в соответствии с требованиями законодательства Российской Федерации).

7.4. Порядок доступа субъекта персональных данных к его персональным данным обрабатываемым Учреждением, определяется в соответствии с законодательством Российской Федерации и локальными актами Учреждения.

7.5. Обработка персональных данных осуществляется:

– с согласия субъекта персональных данных или с согласия его представителя на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных на Учреждение законодательством Российской Федерации функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

7.6. Доступ работников Учреждения к обрабатываемым персональным данным осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

7.7. Допущенные к обработке персональных данных работники Учреждения под роспись знакомятся с документами Учреждения, устанавливающими порядок обработки персональных данных, включая документы, устанавливающие права и обязанности конкретных работников Учреждения.

7.8. Учреждением производится устранение выявленных нарушений законодательства Российской Федерации об обработке и защите персональных данных.

8. Условия обработки персональных данных

8.1. Обработка персональных данных субъектов персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации.

8.2. Обработка персональных данных субъектов персональных данных проходящих медицинские осмотры, медицинские исследования и лечение, а также персональных данных работников Учреждения и иных субъектов персональных данных осуществляется без их согласия в следующих случаях:

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

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

– 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;

– обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях;

– обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

– обработка персональных данных осуществляется при проведении обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований) для определения пригодности работников для выполнения поручаемой работы и предупреждения профессиональных заболеваний.

– обработка персональных данных работников Учреждения осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников Учреждения, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

9. Обеспечение безопасности персональных данных

9.1. Учреждение принимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа, а также иных неправомерных действий в отношении персональных данных.

9.2. Защита персональных данных осуществляется в соответствии с требованиями законодательства Российской Федерации и локальных актов Учреждения. В целях защиты персональных данных Учреждением создана система защиты персональных данных (далее – СЗПД).

9.3. Основными мерами и средствами защиты персональных данных, используемыми Учреждением, являются:

– назначение лица ответственного за обработку персональных данных, которое осуществляет организацию обработки персональных данных, обучение и инструктаж, внутренний контроль за соблюдением Учреждением и ее работниками требований к защите персональных данных;

– определение актуальных угроз безопасности персональных данных при их обработке в ИСПД, и разработка мер и мероприятий по защите персональных данных;

– разработка политики в отношении обработки персональных данных;

– установление правил доступа к персональных данных, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с персональных данных в ИСПД;

– установление индивидуальных паролей доступа работников Учреждения в ИСПД в соответствии с их должностными обязанностями;

– применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей персональных данных, обеспечение их сохранности;

– сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

– сертифицированное программное средство защиты информации от несанкционированного доступа;

– сертифицированные межсетевой экран и средство обнаружения вторжения;

– соблюдение условий, обеспечивающих сохранность персональных данных и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности персональных данных;

– обеспечение регистрации и учета действий, совершаемых с персональных данных, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

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

– обучение работников Учреждения непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

– осуществление внутреннего контроля и аудита;

– иные меры и средства защиты персональных данных, установленные законодательством Российской Федерации.

9.4. Обработка персональных данных в Учреждения ведется:

– с использованием средств автоматизации;

– без использования средств автоматизации.

В соответствии с требованиями Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» Учреждение вправе создавать локальные информационные системы, содержащие данные о пациентах и об оказываемых им медицинских услугах, с соблюдением установленных законодательством Российской Федерации требований о защите персональных данных и соблюдением врачебной тайны.

Автоматизированная обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа, информация доступна лишь для строго определенных работников.

9.5. Доступ работников Учреждения к персональным данным осуществляется только к документам, которые содержат персональные данные субъектов персональных данных, и только для выполнения возложенных на них трудовых и должностных обязанностей, в том объеме, которые необходимы им для выполнения своих должностных обязанностей.

Работники Учреждения, допущенные к обработке персональных данных, информируются об условиях и правилах обработки персональных данных, режимах защиты ИСПД, порядке хранения материальных носителей персональных данных.

Работниками Учреждения даются письменные обязательства о неразглашении персональных данных по форме приложения № 3 к Политике, конфиденциальной информации, а также соблюдении врачебной тайны.

9.6. Обработка и хранение персональных данных осуществляется в следующем порядке:

– персональные данные могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде;

– персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа;

– персональные данные, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках;

– не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках) в ИСПД;

– не допускается хранение и размещение персональных данных на бумажных носителях в не запираемых шкафах и помещениях, порядок доступа к которым имеет неопределенных круг лиц;

– хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

9.7. Уничтожение документов (носителей), содержащих персональных данных производится путем сжигания, дробления (измельчения). Для уничтожения бумажных документов допускается применение шредера.

9.8. Персональных данных на электронных носителях уничтожаются путем стирания или форматирования носителя.

9.9. Уничтожение производится комиссией. Факт уничтожения персональных данных подтверждается документально актом об уничтожении персональных данных, не подлежащих хранению по форме приложения № 5 к Политике (далее – Акт об уничтожении), подписанным членами комиссии.

9.10. Учреждение передает персональных данных третьим лицам в следующих случаях:

– субъект персональных данных выразил свое согласие на такие действия;

– передача персональных данных предусмотрена в рамках установленной законодательством Российской Федерации процедуры.

9.11. Перечень третьих лиц, которым передаются персональных данных:

– Пенсионный фонд Российской Федерации;

– Налоговые органы Российской Федерации;

– Фонд социального страхования;

– Территориальный фонд обязательного медицинского страхования;

– страховые медицинские организации по обязательному и добровольному медицинскому страхованию;

– органы воинского учета;

– банки для начисления заработной платы с согласия субъекта персональных данных;

– Минздрав России с согласия субъекта персональных данных;

– органы, осуществляющие лицензирование;

– прокуратура, иные контролирующие и проверяющие органы;

– судебные и правоохранительные органы;

– бюро кредитных историй, кредитные организации с согласия субъекта персональных данных.

10. Обеспечение конфиденциальности персональных данных при их передаче третьим лицам

10.1. В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федерального закона от 21 ноября 2011 года № 323-ФЗ раскрытие и распространение третьим лицам персональных данных, а также сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, осуществляется с согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

10.2. В соответствии с требованиями статьи Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ передача персональных данных работника третьей стороне осуществляется с его письменного согласия, если иное не предусмотрено законодательством Российской Федерации.

10.3. Передача персональных данных субъектов персональных данных проходящих медицинские осмотры, медицинские исследования и лечение третьим лицам без согласия субъекта персональных данных осуществляется в соответствии с требованиями Федерального закона от 29 ноября 2010 № 326 «Об обязательном медицинском страховании в Российской Федерации» и договорами, заключаемыми субъектами персональных данных либо их работодателем со страховыми компаниями, в целях ведения персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, осуществляется передача сведений о субъекте персональных данных в территориальные фонды ОМС, ДМС, негосударственные страховые компании, и в соответствии с требованиями Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»:

– в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;

– 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 случае оказания медицинской помощи несовершеннолетнему, для информирования одного из его родителей или иного 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;

– 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 целях представления отчетности по видам, формам, в сроки и в объеме, которые установлены уполномоченным федеральным органом исполнительной власти.

10.4. В соответствии с требованиями законодательства Российской Федерации, передача сведений о состоянии здоровья субъекта персональных данных осуществляется в учреждения и организации, в целях организации допуска к исполнению трудовых обязанностей, для посещения детских образовательных учреждений, учреждений дошкольного образования и организаций, занимающихся внешкольной деятельностью с детьми и подростками.

10.5. Передача персональных данных работников Учреждения без их согласия осуществляется в следующих случаях:

– в соответствии с требованиями Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ в случае, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

– в соответствии с требованиями Налогового кодекса Российской Федерации от 05 августа 2000 года № 117-ФЗ представляются в налоговый орган по месту своего учета сведения о доходах физических лиц истекшего налогового периода и суммах начисленных, удержанных и перечисленных в бюджетную систему Российской Федерации за этот налоговый период;

– в соответствии с требованиями Федерального закона от 24 июля 2009 года № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования» представляется отчетность в орган контроля за уплатой страховых взносов по месту своего учета;

– в соответствии с пунктом 5 статьи 19, пункта 1 статьи 21 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» в целях информационного обеспечения пациентов в Учреждении могут создаваться общедоступные источники персональных данных о врачах-специалистах (доска объявлений, информация на сайте и т.п.). В общедоступные источники персональных данных без согласия субъекта персональных данных могут включаться фамилия, имя, отчество, структурное подразделение, должность, сведения о квалификации врача-специалиста, стаж работы.

10.6. Трансграничная передача персональных данных может осуществляться в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных,

и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

– наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

– предусмотренных международными договорами Российской Федерации;

– предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

– исполнения договора, стороной которого является субъект персональных данных;

– защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

10.7. Учреждение вправе на основании заключаемого договора поручить обработку персональных данных другому юридическому лицу или индивидуальному предпринимателю с согласия субъектов персональных данных. Юридическое лицо или индивидуальный предприниматель, осуществляющие обработку персональных данных по поручению Учреждения, обязаны соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации в области персональных данных и обеспечения условий конфиденциальности и безопасности персональных данных при их обработке.

11. Прекращение обработки персональных данных

11.1. Прекращение автоматизированной обработки в ИСПД персональных данных субъектов персональных данных, проходящих медицинские осмотры, медицинские исследования и лечение осуществляется:

– по письменному требованию субъектов персональных данных, немедленно, после завершения производства расчетов за оказанные медицинские и медико-социальные услуги;

– по истечению сроков хранения первичных медицинских документов, установленных законодательством Российской Федерации.

11.2. Прекращение неавтоматизированной обработки персональных данных субъектов, проходящих медицинские осмотры, медицинские исследования и лечение, и уничтожение документов, содержащих персональные данные, осуществляется по истечению сроков хранения первичных медицинских документов, установленных законодательством Российской Федерации, с момента оказания последней медицинской услуги в соответствии с требованиями приказов Министерства здравоохранения и бухгалтерской отчетности.

11.3. Прекращение автоматизированной обработки персональных данных работников Учреждения в ИСПД осуществляется:

– при прекращении договорных отношений с работниками и физическими лицами;

– по истечению сроков представления бухгалтерской отчетности.

11.4. Прекращение неавтоматизированной обработки персональных данных работников Учреждения и уничтожение документов, содержащих персональные данные, осуществляется по истечению сроков хранения документов по личному составу и бухгалтерской отчетности, которые установлены законодательством Российской Федерации, локальными нормативными актами Учреждения.

11.5. Субъект персональных данных (или его представитель) имеет право отозвать согласие на обработку персональных данных по форме приложения № 4 к Политике. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

11.6. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Учреждение осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

12. Порядок блокирования, уничтожения персональных данных.

12.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя, Учреждение обязано осуществить блокировку неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения.

12.2. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя Учреждение обязано осуществить блокировку персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения, если блокировка персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

12.3. В случае подтверждения факта неточности персональных данных, Учреждение на основании сведений, представленных субъектом персональных данных или его представителем, или иных необходимых документов обязано уточнить персональные данные в течение 7 (семи) рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

12.4. В случае выявления неправомерной обработки персональных данных, Учреждение в срок, не превышающий 3 (трех) рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных.

12.5. Если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий 10 (десяти) рабочих дней с даты выявления неправомерной обработки персональных данных, обязана уничтожить такие персональные данные.

12.6. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его представителя.

12.7. В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий 30 (тридцать) дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором либо законодательством Российской Федерации.

12.8. В случае отзыва субъектом персональных данных или его представителем согласия на обработку персональных данных организация обязана прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий 30 (тридцать) дней с даты поступления указанного отзыва, если иное не предусмотрено трудовым договором.

12.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 12.4 – 12.8 Политики, Учреждение осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

13. Порядок уничтожения персональных данных хранящихся на бумажных и электронных (магнитных) носителях.

13.1. Уничтожению подлежат персональные данные хранящиеся на бумажные и электронных (магнитных) носителях, в случае:

– достижения цели обработки персональных данных или утраты необходимости в их обработке;

– выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;

– отзыва субъектом персональных данных согласия на обработку своих персональных данных;

– истечения срока хранения персональных данных.

13.2. Уничтожение производится по мере необходимости, в зависимости от объемов накопленных для уничтожения документов.

13.3. Решение об уничтожении документов, содержащих персональные данные, принимается комиссией по уничтожению персональных данных (далее – Комиссия) в составе не менее 3 (трех) человек.

13.4. Комиссия создается приказом директора Учреждения.

13.5. Основной функцией Комиссии является организация и проведение отбора и подготовки документов, электронных носителей, содержащих персональные данные, к передаче на уничтожение.

13.6. Комиссия производит отбор персональных данных, подлежащих уничтожению, и включает их в акт об уничтожении персональных данных, содержащихся на бумажных и иных носителях, не подлежащих хранению» (приложение № 5 к Политике).

13.7. После этого отобранные документы (электронные носители), отделяются от остальных дел и хранятся в специально отведенном месте до уничтожения. Приготовленные к уничтожению персональные данные (их носители), передаются на переработку специализированной организации или уничтожаются в Учреждения.

13.8. Дела разрешается включать в акт на уничтожение, если их срок хранения закончился. Отбор дел для уничтожения проводится комиссией только с полистным просмотром. После этого документы (электронные носители), отделяются от остальных дел и хранятся в специально отведенном месте до уничтожения.

13.9. Использование персональных данных, включенных в акты об уничтожении, запрещено.

13.10. Комиссия обязана принять решение об уничтожении соответствующих персональных данных в срок, не превышающий трех рабочих дней, с момента их выявления.

13.11. О решении об уничтожении персональных данных Комиссия обязана уведомить субъект персональных данных или его представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

13.12. Ответственным за организацию и проведение мероприятий по уничтожению персональных данных (их носителей) в Учреждения является Комиссия.

13.13. Уничтожение персональных данных делится на два вида:

– плановое уничтожение персональных данных. Уничтожение планируется заранее, отбираются носители с информацией, подлежащей уничтожению, определяется день, место и время уничтожения.

– экстренное уничтожение персональных данных. Уничтожение производится экстренно под воздействием неблагоприятных событий.

13.14. Для уничтожения бумажного носителя используются 2 вида уничтожения:

– уничтожение через шредирование (измельчение и гидрообработка)

– уничтожение через термическую обработку (сжигание).

13.15. Алгоритм уничтожения персональных данных хранящихся на магнитном носителе основывается на многократной перезаписи в секторах магнитного диска. С физической точки зрения, они основываются на многократном перемагничивании материала записывающей поверхности диска. Уничтожение персональных данных с электронных носителей должно производиться согласно стандартам, установленным российскими и международными актами, к примеру: ГОСТ Р50739-95 (РФ), DoD 5220.22-M; NAVSO P-5239-26 (RLL) (США); VSITR (Германия). Алгоритмы национальных стандартов предусматривают запись в каждый байт каждого сектора жесткого диска единиц, случайных чисел, а также чисел, дополнительных к записанным на предыдущем проходе. Предполагается несколько перезаписей для одного материального носителя.

13.16. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности

обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

13.17. При необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

13.18. Уничтожению подвергаются электронные (магнитные) носители, не позволяющие уничтожить или обезличить хранящиеся на них персональные данные методами, указанными в пунктах 3.15 – 3.17 Политики, а также вышедшие из строя электронные (магнитные) носители, на которых осуществлялось хранение персональных данных. Для уничтожения электронного (магнитного) носителя: используется воздействие на рабочие слои дисков, в результате, которого разрушается физическая, магнитная или химическая структура рабочего слоя, а именно:

- механическое разрушение дисков (прессование, механическое эрозирование поверхности, пескоструй, ультразвуковое и электрохимическое эрозирование),
- химическое травление в агрессивных средах
- обжиг или переплавка дисков.

Съём данных с магнитных дисков, подвергшихся таким воздействиям, становится невозможным.

14. Основные права субъекта персональных данных

14.1. Субъект персональных данных имеет право (сам или через представителей) на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Учреждение способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основаниях, предусмотренных действующим законодательством Российской Федерации;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Законом № 152-ФЗ;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Законом № 152-ФЗ или другими федеральными законами.

14.2. Субъект персональных данных или его представитель вправе требовать от Учреждения уточнения персональных данных субъекта 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.

14.3. Субъект персональных данных или его представитель вправе требовать от Учреждения извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

14.4. Субъект персональных данных или его представитель вправе обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

14.5. Субъект персональных данных, сам или через своего представителя, вправе требовать защиты своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

15. Основные права и обязанности Учреждения.

15.1. Учреждения, как оператор персональных данных, вправе:

– отстаивать свои интересы в суде;

– передавать и раскрывать персональные данные субъектов третьим лицам, в случаях и порядке, предусмотренных законодательством Российской Федерации;

– отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством Российской Федерации;

– использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством Российской Федерации

15.2. Учреждение обязано:

– при сборе персональных данных предоставить субъекту или его представителю информацию об обработке персональных данных субъекта;

– в случаях если персональных данных были получены не от субъекта персональных данных и не от его представителя уведомить субъекта персональных данных или его представителя;

– при отказе в предоставлении персональных данных субъекту или его представителю разъяснить последствия такого отказа;

– 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;

– принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

– давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.

16. Заключительные положения

16.1. Политика является внутренним документом Учреждения, общедоступным и подлежит размещению на официальном сайте: www.nczd.ru.

16.2. Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.

16.3. Контроль исполнения требований Политики осуществляется лицом из числа работников Учреждения, назначенным ответственным за организацию обработки персональных данных.

16.4. Ответственность должностных лиц Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Учреждения.

ПРИЛОЖЕНИЕ № 1
к Политике обработки и защиты
персональных данных

Перечень персональных данных, подлежащих защите.

Настоящий Перечень персональных данных, подлежащих защите в Учреждение, разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Перечень содержит полный список категорий данных, безопасность которых должна обеспечиваться СЗПД.

1. Общие положения

1.1. Объектами защиты являются – информация, обрабатываемая в ИСПД, и технические средства ее обработки и защиты.

1.2. Объекты защиты каждой ИСПД включают:

1.2.1. Обрабатываемая информация:

- персональные данные пациентов Учреждения (раздел 2.1.1);
- персональные данные физических лиц, состоящих с Учреждения в трудовых отношениях (раздел 2.1.2);
- персональные данные физических лиц, являющихся представителями пациентов (2.1.3);
- персональные данные детей работников Учреждения в связи с оформлением льгот в соответствии с требованиями законодательства Российской Федерации (2.1.4);
- персональные данные физических лиц, являющихся близкими родственниками работников Учреждения (2.1.5);
- персональные данные физических лиц, уволившихся из Учреждения, в объеме, необходимом для соблюдений требования законодательства Российской Федерации (2.1.6);
- персональные данные физических лиц в связи с гражданско-правовыми отношениями с Учреждения (2.1.7);
- персональные данные работников юридических лиц, являющихся контрагентами Учреждения, необходимые для выполнения своих обязательств в рамках договорных отношений с контрагентом и для выполнения требований законодательства Российской Федерации (2.1.8);
- персональные данные посетителей в связи с контрольно-пропускным режимом (2.1.9);

1.2.2. Технологическая информация (раздел 2.2).

1.2.3. Программно-технические средства обработки (раздел 2.3).

1.2.4. Средства защиты персональных данных (раздел 2.4).

1.2.5. Каналы информационного обмена и телекоммуникации (раздел 2.5).

1.2.6. Объекты и помещения, в которых размещены компоненты ИСПД (раздел 2.6).

2. ИСПД Учреждения

2.1. Обрабатываемая информация

2.1.1. Перечень персональных данных физических лиц, которым оказывается

медицинская помощь:

– фамилия, имя, отчество (последнее - при наличии); пол; дата рождения; место рождения;

– гражданство; данные документа, удостоверяющего личность;

– место жительства; место регистрации; дата регистрации;

– страховой номер индивидуального лицевого счета (при наличии), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования (СНИЛС);

– сведения о составе семьи, фамилии, имена, отчества, даты рождения, адреса прописки и проживания, телефоны, место работы или учебы, занимаемая должность родителей, иных представителей;

– свидетельство о рождении;

– номер полиса обязательного медицинского страхования застрахованного лица (при наличии); номер полиса ДМС;

– справка МСЭ;

– наименование посещаемого образовательного учреждения (МДОУ, школы, ПУ, ССУЗ, ВУЗ), в том числе номер группы, класса, курса;

– анамнез, диагноз;

– сведения об организации, оказавшей медицинские услуги;

– вид оказанной медицинской помощи; условия оказания медицинской помощи;

– сроки оказания медицинской помощи; объем оказанной медицинской помощи;

– результат обращения за медицинской помощью;

– серия и номер выданного листка нетрудоспособности (при наличии);

– сведения об оказанных медицинских услугах; примененные стандарты медицинской помощи;

– сведения о медицинском работнике или медицинских работниках, оказавших медицинскую услугу.

2.1.2. Перечень персональных данных физических лиц, состоящих с Учреждением в трудовых отношениях:

– фамилия, имя, отчество;

– прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

– пол, возраст;

– дата и место рождения;

– гражданство;

– паспортные данные (серия, номер, код подразделения, когда и кем выдан);

– данные паспорта, удостоверяющего личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, когда и кем выдан);

– адрес регистрации по месту жительства и адрес фактического проживания;

– дата регистрации по месту жительства;

– адрес электронной почты;

– номер телефона (домашний, мобильный);

– идентификационный номер налогоплательщика;

– данные страхового свидетельства обязательного пенсионного страхования;

– данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;

– данные о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученой степени, ученом звании (когда присвоены, номера дипломов, аттестатов);

– государственные награды, иные награды и знаки отличия (кем награжден и когда);

– допуск к государственной тайне, оформленный за период работы (форма, номер и дата);

– сведения о наличии (отсутствии) судимости;

– сведения о наличии (отсутствии) заболевания, препятствующего поступлению на работу или ее выполнению, подтвержденного заключением медицинского учреждения;

– результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований);

– отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

– сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

– информация о приеме, переводах, увольнении и иных событиях, относящихся к трудовой деятельности в Учреждении;

– семейное положение (по необходимости);

– сведения о членах семьи, степень родства, фамилии, имена, отчества, даты рождения, в случае оказания родственникам медицинских услуг в Учреждении, а также для предоставления льгот, предусмотренных трудовым и налоговым законодательством Российской Федерации, коллективным договором, локальными нормативно-правовыми актами, приказами и распоряжениями Министерства здравоохранения Российской Федерации;

2.1.3. Перечень персональных данных физических лиц, являющихся представителями пациентов, физических лиц:

– фамилия, имя, отчество;

– паспортные данные (серия, номер, код подразделения, когда и кем выдан, адрес регистрации);

– данные свидетельства о рождении и иных документов, подтверждающих права представителей.

2.1.4. Перечень персональных данных детей работников Учреждения:

– фамилия, имя, отчество;

– паспортные данные (серия, номер, код подразделения, когда и кем выдан, адрес регистрации);

– данные свидетельства о рождении и иных документов, подтверждающих права представителей, работников Учреждения.

2.1.5. Перечень персональных данных физических лиц, являющихся близкими родственниками работников Учреждения:

– фамилия, имя, отчество;

– данные, подтверждающие степень родства;

– данные, необходимые для внесения в личную учетную карточку Т-2 работника Учреждения;

– данные, необходимые для определения и назначения необходимых льгот.

2.1.6. Перечень персональных данных физических лиц, уволившихся из Учреждения:

– фамилия, имя, отчество;

– прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

– пол, возраст;

– дата и место рождения;

– гражданство;

– паспортные данные (серия, номер, код подразделения, когда и кем выдан);

– данные паспорта, удостоверяющего личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, когда и кем выдан);

– адрес регистрации по месту жительства и адрес фактического проживания;

– дата регистрации по месту жительства;

– адрес электронной почты;

– номер телефона (домашний, мобильный);

– идентификационный номер налогоплательщика;

– данные страхового свидетельства обязательного пенсионного страхования;

– данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;

– данные о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученой степени, ученом звании (когда присвоены, номера дипломов, аттестатов);

– государственные награды, иные награды и знаки отличия (кем награжден и когда);

– допуск к государственной тайне, оформленный за период работы (форма, номер и дата);

– сведения о наличии (отсутствии) судимости;

– сведения о наличии (отсутствии) заболевания, препятствующего поступлению на работу или ее выполнению, подтвержденного заключением медицинского учреждения;

– результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований);

– отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

– сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

– информация о приеме, переводах, увольнении и иных событиях, относящихся к трудовой деятельности в Учреждении;

– семейное положение (по необходимости);

2.1.7. Перечень персональных данных физических лиц в связи с гражданско-правовыми отношениями с Учреждения:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- паспортные данные (серия, номер, код подразделения, когда и кем выдан);
- адрес регистрации по месту жительства и адрес фактического проживания;
- дата регистрации по месту жительства;
- адрес электронной почты;
- номер телефона (домашний, мобильный);
- идентификационный номер налогоплательщика;
- данные страхового свидетельства обязательного пенсионного страхования;

2.1.8. Перечень персональных данных работников юридических лиц, являющихся контрагентами Учреждения, необходимые для выполнения ими своих обязательств в рамках договорных отношений с контрагентом и для выполнения требований законодательства Российской Федерации:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- паспортные данные (серия, номер, код подразделения, когда и кем выдан);
- адрес регистрации по месту жительства и адрес фактического проживания;
- дата регистрации по месту жительства;
- адрес электронной почты;
- номер телефона (домашний, мобильный);

2.1.9. Перечень персональные данные посетителей в связи с контрольно-пропускным режимом:

- фамилия, имя, отчество;
- дата и место рождения;
- гражданство;
- паспортные данные (серия, номер, код подразделения, когда и кем выдан);
- адрес регистрации по месту жительства;
- дата регистрации по месту жительства;

2.2. Технологическая информация

Технологическая информация, подлежащая защите, включает:

- управляющую информацию (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическую информацию средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информацию на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащих защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информацию о СЗПД, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие

информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

– служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки обрабатываемой информации.

2.3. Программно-технические средства

Программно-технические средства включают в себя:

– общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);

– резервные копии общесистемного программного обеспечения;

– инструментальные средства и утилиты систем управления ресурсами ИСПД;

– аппаратные средства обработки персональных данных (АРМ и сервера);

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

2.4. Средства защиты персональных данных

Средства защиты персональных данных состоят из аппаратно-программных средств и включают в себя:

– средства управления и разграничения доступа пользователей;

– средства обеспечения регистрации и учета действий с информацией;

– средства, обеспечивающие целостность данных;

– средства антивирусной защиты;

– средства межсетевого экранирования;

– средства анализа защищенности;

– средства обнаружения вторжений;

– средства криптографической защиты персональных данных, при их передаче по каналам связи.

2.5. Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.6. Объекты и помещения, в которых размещены компоненты ИСПД

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

ПРИЛОЖЕНИЕ № 2
к Политике обработки и защиты
персональных данных
ФГАУ «НМИЦ здоровья детей»
Минздрава России

Согласие на обработку персональных данных работника

Я, _____, паспорт серии_____, номер _____, выданный _____ «__» _____ _____ г. Проживающий по адресу _____, поступая на работу в ФГАУ «НМЦ здоровья детей» Минздрава России в должность _____, в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты, предусмотренных законодательством Российской Федерации налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством Российской Федерации отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд Российской Федерации, сведений подоходного налога в ФНС России, сведений в ФСС Российской Федерации;
- предоставления сведений в банк для оформления банковской карты и перечисления на нее заработной платы;
- предоставления сведений третьим лицам для оформления полиса ДМС;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности имущества работодателя
- даю согласие ФГАУ «НМЦ здоровья детей» Минздрава России, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;

– адрес регистрации по месту жительства и адрес фактического проживания;
– номер телефона (домашний, мобильный);
– данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
– семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством Российской Федерации;
– отношение к воинской обязанности;
– сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
– сведения об образовании, профессиональной подготовке, переподготовке и повышении квалификации;
– СНИЛС;
– ИНН;
– информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ФГАУ «НМЦ здоровья детей» Минздрава России;
– сведения о доходах в ФГАУ «НМЦ здоровья детей» Минздрава России;
– сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме. Отзыв направляется работодателю заказным письмом с уведомлением о получении. Отзыв на обработку персональных данных может быть передан работодателю мною лично или моим доверенным лицом, полномочия которого устанавливаются доверенностью, заверенной нотариально.

Срок, в течение которого действует настоящее согласие, определяется сроком моих трудовых отношений с ФГАУ «НМЦ здоровья детей» Минздрава России и сроками хранения архивных документов, определенных законодательством Российской Федерации.

Порядок отзыва согласия на обработку персональных данных и его возможности последствия мне разъяснены.

«___» _____ 201__ года

Подпись _____/_____

ПРИЛОЖЕНИЕ № 3
к Политике обработки и защиты
персональных данных
ФГАУ «НМИЦ здоровья детей»
Минздрава России

Обязательство о неразглашении персональных данных субъектов

Я, _____, должность _____, обязуюсь не разглашать персональные данные работников, вставшие мне известными в связи с исполнением своих должностных обязанностей.

Я подтверждаю, что без письменного согласия субъекта персональных данных, не имею права разглашать и передавать третьим лицам:

- анкетных и биографических данных;
- образования;
- сведений о трудовом стаже;
- сведений о составе семьи;
- паспортных данных;
- сведений о воинском учете;
- сведений о заработной плате;
- сведений о социальных льготах;
- специальности;
- занимаемой должности;
- наличия судимостей;
- адреса места жительства;
- домашнего телефона;
- мобильного телефона;
- адреса электронной почты;
- содержания трудового договора;
- содержания декларации, подаваемой в налоговую инспекцию;
- подлинников и копии приказов по личному составу;
- личного дела и трудовой книжки;
- оснований к приказам по личному составу;
- материалов по повышению квалификации и переподготовке;
- аттестаций и материалов к служебным расследованиям;
- отчетов, направляемых в органы статистики;
- врачебную тайну.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации, ст. 24 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

С Политикой обработки и защиты персональных данных ФГАУ «НМИЦ здоровья детей» Минздрава России ознакомлен(а).

«___» _____ 201__ года

Подпись _____/_____

ПРИЛОЖЕНИЕ № 4
к Политике обработки и защиты
персональных данных
ФГАУ «НМИЦ здоровья детей»
Минздрава России

Отзыв согласия на обработку персональных данных.

ФГАУ директору «НМЦ здоровья детей»
Минздрава России

_____
(Ф.И.О.)

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

Прошу Вас прекратить обработку моих персональных данных с _____ 20____года

«___» _____ 20____ года _____/_____

ПРИЛОЖЕНИЕ № 5
к Политике обработки и защиты
персональных данных
ФГАУ «НМИЦ здоровья детей»
Минздрава России

АКТ №_____от «__» _____ 20___г____
об уничтожении персональных данных, содержащихся на бумажных и иных носителях, не подлежащих хранению

Комиссия в составе:
Председатель _____
Члены комиссии_____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ _____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/н	Заголовок документа	Дата	Регистрационный номер носителя	Кол-во ед. хранения	Примечание/тип носителя

Всего съемных носителей _____
_____

На указанных носителях персональные данные уничтожены путем_____
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных уничтожены путем _____
_____.
(разрезания, сжигания, механического уничтожения, форматирования и т.п.)

Председатель комиссии: _____

Члены комиссии:
1. _____ (должность, ФИО)
2. _____ (должность, ФИО)
3. _____ (должность, ФИО)
4. _____ (должность, ФИО)