УТВЕРЖДАЮ
Директор Томского НИМЦ

_____ В.А. Степанов

2019 г.

ПОЛИТИКА

в отношении обработки персональных данных
Федерального государственного бюджетного научного учреждения
«Томский национальный исследовательский медицинский центр
Российской академии наук»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Общие положения

Настоящий документ в отношении обработки персональных данных (далее – Политика) разработан в соответствии с пп. 2 п.1 статьи 18.1 Федерального закона от 27 июля 2006 года № 152 «О персональных данных» и определяет цели и общие принципы в отношении действий (операций) по обработке и защите персональных данных в Федеральном государственном бюджетном научном учреждении «Томский национальный исследовательский медицинский центр Российской академии наук» (далее - Оператор).

1.2. В настоящей Политике используются следующие основные понятия и определения:

Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (Субъекту персональных данных).

Информация - сведения (сообщения, данные) независимо от формы их представления.

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), трансграничную передачу, обезличивание, блокирование, удаление, уничтожение Персональных данных.

Автоматизированная обработка персональных данных - Обработка персональных данных с помощью средств вычислительной техники.

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое 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.

Субъект персональных данных - физическое лицо, к которому прямо или косвенно относятся соответствующие Персональные данные.

Информационная система персональных данных - совокупность содержащихся в базах данных Персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязанность Оператора персональных данных и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством.

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

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

Блокирование персональных данных - временное прекращение Обработки персональных данных (за исключением случаев, если обработка необходима для уточнения Персональных данных).

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

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

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность Персональных данных конкретному Субъекту персональных данных.

1.3. Область действия

Действие настоящей Политики распространяется на все процессы Оператора, в рамках которых осуществляется Обработка персональных данных, как с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и без использования таких средств.

Настоящая Политика распространяется на все структурные подразделения и филиалы Оператора.

Настоящая Политика обязательна для ознакомления и исполнения всеми лицами, допущенными Оператором к Обработке персональных данных, и лицами, участвующими в организации процессов Обработки персональных данных и обеспечения безопасности Персональных данных.

Для реализации целей настоящей Политики Оператор может разрабатывать и утверждать соответствующие положения, регламенты, руководства, приказы и иные локальные нормативные акты.

1.4. Утверждение и пересмотр

Настоящая Политика вступает в силу с момента ее утверждения Директором Оператора и действует бессрочно до замены ее новой Политикой. Обеспечение неограниченного доступа к Политике реализуется путем ее публикации на сайте Оператора в сети Интернет.

2. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор производит обработку только тех персональных данных, которые необходимы для выполнения фундаментальных, посковых и прикладных (в том числе клинических) научных исследований, направленных на изучение этиопатогенеза основных социально-значимых заболеваний, разработку и внедрение технологий опережающего развития в фундаментальной и клинической медицине и лекарственных средств с использованием уникального научно-образовательного потенциала, для повышения эффективности медицинской помощи населению Российской Федерации, а также в целях исполнения требований законодательства РФ.

3. ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Правовыми основаниями обработки Оператором персональных данных в порядке, предусмотренном настоящей Политикой, являются:

- Трудовой кодекс Российской Федерации;

- Налоговый кодекс Российской Федерации;
- Федеральный закон "Об обязательном медицинском страховании в Российской Федерации" от 29.11.2010 №326-ФЗ;
- Федеральный закон "Об основах охраны здоровья граждан в Российской Федерации" от 21.11.2011 №323-ФЗ;
- Федеральный закон «О бухгалтерском учете» от 06.12.2011 №402-ФЗ;
- Федеральный закон «Об архивном деле в Российской Федерации» от 22.10.2004 №125-ФЗ;
- иные нормативно-правовые актов Российской Федерации, в рамках осуществления и выполнения, возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;
- учредительные документы Оператора;
- заключаемые Оператором гражданско-правовые и иные договоры и соглашения;
- согласия Субъектов персональных данных на обработку персональных данных.

4. ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.

Оператором может производиться Обработка персональных данных следующих категорий Субъектов персональных данных:

- физические лица – работники Оператора;
- физические лица – представители работников Оператора;
- физические лица – родственники работников Оператора;
- физические лица – кандидаты, рассматриваемые Оператором с целью заключения трудовых договоров;
- физические лица – работники контрагентов и третьих лиц;
- физические лица – пациенты Оператора;
- физические лица – представители пациентов Оператора;
- физические лица – родственники пациентов Оператора;
- физические лица – посетители помещений Оператора;
- физические лица, заключившие гражданско-правовые договоры с Оператором;
- физические лица, состоявшие ранее в трудовых отношениях с Оператором;
- авторы письменных и иных обращений в адрес Оператора;
- иные Субъекты персональных данных (для обеспечения реализации целей Обработки, указанных в разделе 2 Политики).

Перечень и объем Персональных данных, обрабатываемых Оператором, определяется в соответствии с законодательством Российской Федерации, локальными нормативными актами Оператора и подготавливаемыми на их основании документами отдельно для каждого процесса, связанного с Обработкой персональных данных, с учетом целей Обработки персональных данных, указанных в разделе 2 Политики.

5. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Общий порядок обработки

При организации обработки персональных данных Оператором выполняются следующие принципы и условия:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность и актуальность по отношению к целям обработки персональных данных;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки.
- персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Оператор в своей деятельности исходит из того, что субъект персональных данных предоставляет точную и достоверную информацию, во время взаимодействия с Оператором извещает представителей Оператора об изменении своих персональных данных.

5.2. Перечень действий с Персональными данными и способы Обработки персональных данных

Оператор может осуществлять обработку Персональных данных в т.ч.: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), трансграничную передачу, обезличивание, блокирование, удаление, уничтожение.

Обработка персональных данных осуществляется Оператором следующими способами:

- Неавтоматизированная Обработка персональных данных;
- Автоматизированная Обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;

- Смешанная Обработка персональных данных.

5.3. Условия Обработки персональных данных Субъектов персональных данных и ее передачи третьим лицам

Оператор обрабатывает и хранит персональные данные субъектов в соответствии с внутренними нормативными документами, разработанными согласно законодательству РФ.

Порядок и сроки хранения Персональных данных, обрабатываемых Оператором, определяются в соответствии с законодательством Российской Федерации, локальными нормативными актами Оператора и подготавливаемыми на их основании документами отдельно для каждого процесса, связанного с Обработкой персональных данных, с учетом целей Обработки персональных данных, указанных в разделе 2 Политики.

В отношении персональных данных субъекта обеспечивается их конфиденциальность, целостность и доступность. Передача персональных данных третьим лицам для выполнения договорных обязательств осуществляется только с согласия субъекта персональных данных, а для выполнения требований законодательства РФ – в рамках установленной законодательством процедуры. В случае реорганизации, продажи или иной передачи бизнеса (полностью или части) Оператора к приобретателю переходят все обязательства по соблюдению условий настоящей Политики применительно к получаемым им персональным данным.

Оператор может поручить обработку персональных данных другому лицу при выполнении следующих условий:

- получено согласие субъекта на поручение обработки персональных данных другому лицу;

- поручение обработки персональных данных осуществляется на основании заключаемого с этим лицом договора, разработанного с учетом требований Федерального закона РФ от 27 июля 2006 года № 152 «О персональных данных»;

- иных случаях, предусмотренных действующим законодательством.

Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных и несет ответственность перед Оператором. Оператор несет ответственность перед субъектом персональных данных за действия уполномоченного лица, которому Оператор поручил обработку персональных данных.

6. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Субъект персональных данных имеет право на получение информации, касающейся Обработки персональных данных, в том числе содержащей:

- подтверждение факта Обработки персональных данных Оператором;

- правовые основания и цели Обработки персональных данных;

- цели и применяемые Оператором способы Обработки персональных данных;

- наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к Персональным данным

или которым могут быть раскрыты Персональные данные на основании договора с Оператором или на основании Федерального закона;

- 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 настоящим Федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего Обработку персональных данных по поручению Оператора, если Обработка персональных данных поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими Федеральными законами.

Право Субъекта персональных данных на доступ к его Персональным данным может быть ограничено в соответствии с действующим законодательством.

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

3. Если Субъект персональных данных считает, что Оператор осуществляет Обработку персональных данных с нарушением требований действующего законодательства или иным образом нарушает его права и свободы, то Субъект персональных данных вправе обжаловать действия или бездействие Оператора в порядке, предусмотренном действующим законодательством.

7. ОБЯЗАННОСТИ ОПЕРАТОРА

В соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных» Оператор обязан:

1. Осуществлять Обработку персональных данных с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;

2. Не раскрывать третьим лицам и не распространять персональные данные без согласия Субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ «О персональных данных»;

3. Предоставить доказательство получения согласия Субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, в соответствии с которыми такое согласие не требуется;

4. В случаях, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных», осуществлять Обработку персональных данных только с согласия в письменной форме Субъекта персональных данных;

5. Предоставлять Субъекту персональных данных по его запросу информацию, касающуюся Обработки персональных данных, либо на законных основаниях предоставить отказ в предоставлении указанной информации и дать в письменной форме мотивированный ответ, содержащий ссылку на положения Федерального закона № 152-ФЗ «О персональных данных», являющееся основанием для такого отказа, в порядке и сроки, предусмотренные действующим законодательством, настоящей Политикой и иными локальными нормативными актами Оператора.

6. Если предоставление персональных данных является обязательным в соответствии с Федеральным законом, разъяснить Субъекту персональных данных юридические последствия отказа предоставить его Персональные данные;

7. 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. Описание принимаемых мер приведено в разделе 6 настоящей Политики;

8. При сборе Персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение Персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев предусмотренном действующим законодательством.

9. По требованию Субъекта персональных данных внести изменения в обрабатываемые Персональные данные, или уничтожить их, если Персональные данные являются неполными, неточными, неактуальными, незаконно полученными или не являются необходимыми для заявленной цели в порядке и сроки, предусмотренные действующим законодательством, настоящей Политикой и иными локальными нормативными актами Оператора.

10. Организовывать прием и обработку обращений и запросов Субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов. В т.ч. в этих целях Оператор вправе вести «Журнал учета обращений субъектов персональных данных», в котором должны фиксироваться запросы Субъектов персональных данных на получение Персональных данных, а также факты предоставления Персональных данных по этим запросам.

11. Уведомлять Субъекта персональных данных об Обработке персональных данных в том случае, если Персональные данные были получены не от Субъекта персональных данных. Исключение составляют следующие случаи:

- Субъект персональных данных уведомлен об осуществлении Обработки персональных данных Оператором;

- Персональные данные получены Оператором на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект персональных данных;
- Персональные данные сделаны общедоступными Субъектом персональных данных или получены из общедоступного источника;
- Оператор осуществляет Обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы Субъекта персональных данных;
- предоставление Субъекту персональных данных сведений, содержащихся в уведомлении об обработке персональных данных, нарушает права и законные интересы третьих лиц.

12. В случае выявления неправомерной Обработки персональных данных или неточных Персональных данных, устранить выявленные нарушения в соответствии с порядком и сроками, установленными Федеральным законом № 152-ФЗ «О персональных данных».

13. В случае достижения целей Обработки персональных данных незамедлительно прекратить Обработку персональных данных и уничтожить соответствующие Персональные данные в срок, не превышающий тридцати дней с даты достижения цели Обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект персональных данных, иным соглашением между Оператором и Субъектом персональных данных (в т.ч. соответствующим согласием Субъекта персональных данным на Обработку персональных данных) либо если Оператор не вправе осуществлять Обработку персональных данных без согласия Субъекта персональных данных на основаниях, предусмотренных №152-ФЗ «О персональных данных» или другими Федеральными законами.

14. В случае отзыва Субъектом персональных данных согласия на Обработку своих персональных данных прекратить Обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и Субъектом персональных данных либо действующим законодательством. Об Уничтожении персональных данных Оператор обязан уведомить Субъекта персональных данных.

8. МЕРЫ, ПРИМЕНЯЕМЫЕ ОПЕРАТОРОМ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор принимает необходимые и достаточные организационные и технические меры для защиты персональных данных субъектов от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ней третьих лиц.

К основным методам и способам обеспечения безопасности персональных данных относятся:

1. Назначение Оператором, лица, ответственного за организацию Обработки персональных данных.

2. Издание Оператором, документов, определяющих политику Оператора в отношении Обработки персональных данных, локальных актов по вопросам Обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

3. Применение правовых, организационных и технических мер по обеспечению безопасности Персональных данных в соответствии действующим законодательством, в том числе:

- определение угроз безопасности Персональных данных при их обработке в Информационных системах персональных данных;
- применение организационных и технических мер по обеспечению безопасности Персональных данных при их обработке в Информационных системах персональных данных, необходимых для выполнения требований к защите Персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценка эффективности принимаемых мер по обеспечению безопасности Персональных данных до ввода в эксплуатацию Информационной системы персональных данных;
- учет машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к Персональным данным и принятием мер;
- восстановление Персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к Персональным данным, обрабатываемым в Информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с Персональными данными в Информационной системе персональных действий, совершаемых с Персональными данными в Информационной системе персональных данных;
- контроль за принимаемыми мерами по обеспечению безопасности Персональных данных и уровня защищенности информационных систем персональных данных.

4. Осуществление внутреннего контроля и (или) аудита соответствия Обработки персональных данных действующему законодательству, требованиям к защите

Персональных данных, политике Оператора в отношении Обработки персональных данных, локальным актам Оператора.

5. Оценка вреда, который может быть причинен Субъектам персональных данных в случае нарушения действующего законодательства, соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством.

6. Ознакомление работников Оператора, непосредственно осуществляющих Обработку персональных данных, с положениями законодательства Российской Федерации о Персональных данных, в том числе требованиями к защите Персональных данных, документами, определяющими политику Оператора в отношении Обработки персональных данных, локальными актами по вопросам Обработки персональных данных, и (или) обучение указанных работников.

7. Обеспечение неограниченного доступа к документу, определяющему политику Оператора в отношении Обработки персональных данных, к сведениям о реализуемых требованиях к защите Персональных данных. Опубликование в соответствующих информационно-телекоммуникационных сетях документа, определяющий политику Оператора в отношении Обработки персональных данных, и сведения о реализуемых требованиях к защите Персональных данных, а также обеспечение возможности доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

8. Оператор вправе принимать иные меры необходимые для защиты Персональных данных в соответствии с действующим законодательством и локальными нормативными актами Оператора.