УТВЕРЖДЕНА
приказом ФГБУ «НМИЦ онкологии
им. Н.Н. Блохина» Минздрава России
от «29» 04 2021 г. № 260/п

# Политика обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России

## 1. Общие положения

1.1. Политика обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России (далее — Политика) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни обрабатываемых в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России (далее – Учреждение) персональных данных, субъектов персональных данных и их права, функции Учреждения при обработке персональных данных, а также реализуемые в Учреждении требования к защите персональных данных.

1.2. Положения Политики служат основой для разработки локальных нормативных актов, регламентирующих вопросы обработки персональных данных работников Учреждения и других субъектов персональных данных.

## 2. Законодательные и иные правовые акты Российской Федерации, в соответствии с которыми определяется Политика обработки персональных данных в Учреждении

2.1. Политика обработки персональных данных в Учреждении определяется в соответствии со следующими правовыми актами:

– Трудовой кодекс Российской Федерации;

– Гражданский кодекс Российской Федерации;

– Налоговый кодекс Российской Федерации;

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Федеральный закон от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

– Федеральный закон от 28 марта 1998 г. № 53-ФЗ «О воинской обязанности и военной службе»;

– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 06 декабря 2011 г. № 402-ФЗ «О бухгалтерском учете»;

– Федеральным законом от 29.11.2010 N 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

– Федеральный закон от 21.11.2011 N 323-ФЗ (ред. от 02.07.2021) «Об основах охраны здоровья граждан в Российской Федерации»;

– Постановление Правительства РФ от 04.10.2012 N 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;

– Указ Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

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

– Постановление Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 27 ноября 2006 г. №719 «Об утверждении Положения о воинском учете»;

– Поручение Председателя Правительства Российской Федерации от 28 ноября 2011 г. № ВП-П13-9308 «О сборе информации обо всей цепочке собственников контрагентов, включая бенефициаров»;

– приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изм. от 23.03.2017);

– Приказ Роскомнадзора от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

– Устав ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России;

– Антикоррупционная политика ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России;

– согласие на обработку персональных данных;

– иные нормативные правовые акты Российской Федерации, нормативные документы уполномоченных органов государственной власти.

2.2. В целях реализации положений Политики в Учреждении разрабатываются соответствующие локальные нормативные акты, регламентирующие вопросы обработки персональных данных.

## 3. Основные термины и определения

Персональные данные — любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Специальные категории персональных данных — сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, судимости.

Биометрические персональные данные — сведения, которые характеризуют физиологические и биологические особенности человека (в том числе изображение

человека — фотография и видеозапись), на основании которых можно установить его личность и которые используются структурными подразделениями ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России для установления личности субъекта персональных данных.

Общедоступные персональные данные — персональные данные, в частности фамилия, имя, отчество, фотография, место работы, занимаемая должность, рабочий телефон, служебный адрес электронной почты, которые с письменного согласия субъекта персональных данных включены в общедоступные источники персональных данных (справочники).

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

Оператор — 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.

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

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств автоматизации.

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

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

Разглашение персональных данных — действия (бездействие), в результате которых персональные данные в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становятся известными третьим лицам без письменного согласия субъекта персональных данных, за исключением случаев, предусмотренных федеральным законодательством.

Доступ к персональным данным — возможность получения персональных данных и их использование.

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

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

Уничтожение персональных данных — действия, в результате которых

становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных — информационная система, предназначенная для обработки персональных данных.

## 4. Принципы и цели обработки персональных данных

4.1. Учреждение, являясь оператором, осуществляет обработку персональных данных работников, пациентов и других субъектов персональных данных, не состоящих с Учреждением в трудовых отношениях.

4.2. Обработка персональных данных в Учреждении осуществляется с учетом необходимости обеспечения защиты прав и свобод работников, пациентов и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

– обработка персональных данных осуществляется в Учреждении на законной и справедливой основе;

– обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

– не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– 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;

– содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки, не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

– при обработке персональных данных обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждением принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

– хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект

персональных данных;

– обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Персональные данные обрабатываются в целях:

– обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Учреждения;

– осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Учреждение, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, а также в иные государственные органы;

– регулирования трудовых отношений с работниками Учреждения (содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы, обеспечение сохранности имущества);

– оказания медицинских услуг пациентам Учреждения;

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

– подготовки, заключения, исполнения и прекращения договоров с контрагентами;

– осуществления образовательной деятельности;

– осуществления деятельности, связанной с правовой охраной и использованием результатов интеллектуальной деятельности Учреждения;

– осуществления издательской деятельности;

– организации и проведения конференций, симпозиумов, семинаров, выставок и других научных и научно-организационных мероприятий;

– оказания гостиничных услуг;

– осуществления деятельности по заготовке донорской крови;

– осуществления деятельности по забору органов и (или) тканей человека для трансплантации;

– обеспечения пропускного и внутриобъектового режимов на объектах Учреждения;

– формирования справочных материалов для внутреннего информационного обеспечения деятельности Учреждения;

– исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации, в т. ч. в соответствии с законодательством об исполнительном производстве;

– осуществления прав и законных интересов Учреждения в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами;

– противодействия коррупции;

– в иных законных целях.

## 5. Перечень субъектов, персональные данные которых обрабатываются в Учреждении

В Учреждении обрабатываются персональные данные следующих категорий субъектов:

– работники структурных подразделений;

– кандидаты на замещение вакантных должностей;

– лица, наделенные правом подписи от имени Учреждения (договоров, контрактов, соглашений, актов и т.д.);

– пациенты/контрагенты (физические лица);

– физические лица в цепочке собственников контрагентов Учреждения;

– физические лица, направляющие обращения в Учреждение;

– другие субъекты персональных данных (для обеспечения реализации целей обработки, указанных в разделе 4.3 Политики).

## 6. Перечень персональных данных, обрабатываемых в Учреждении

6.1. Перечень персональных данных, обрабатываемых в Учреждении, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Учреждения, с учетом целей обработки персональных данных, указанных в разделе 4.3 Политики.

6.2. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Учреждении не производится.

## 7. Функции Учреждения при осуществлении обработки персональных данных

Учреждение при осуществлении обработки персональных данных:

– принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Учреждения, в области персональных данных;

– принимает правовые, организационные и технические меры 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;

– назначает лицо, ответственное за организацию обработки персональных данных в Учреждении;

– издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных;

– осуществляет ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Учреждения в области персональных

данных, в том числе требованиями к защите персональных данных, и обучение указанных работников;

– публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;

– сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

– назначает работника в Учреждении, ответственного за прием обращений и запросов субъектов персональных данных;

– не сообщает, не раскрывает третьим лицам и не распространяет персональные данные без согласия работников Учреждения и других субъектов персональных данных, за исключением случаев, 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 и нормативно-правовыми актами;

– разъясняет порядок защиты субъектом персональных данных своих прав и законных интересов;

– разъясняет работникам Учреждения, пациентам/контрагентам и другим субъектам персональных данных юридические последствия отказа предоставить свои персональные данные в случае, если предоставление персональных данных является обязательным в соответствии с законодательством Российской Федерации;

– в случае подтверждения факта неточности персональных данных уточняет персональные данные или обеспечивает их уточнение;

– блокирует персональные данные на период внутренней проверки в случае выявления:

– неправомерной обработки персональных данных;

– неточных персональных данных;

– прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

– совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

## 8. Условия обработки персональных данных

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

8.2. Учреждение без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не

предусмотрено действующим законодательством.

8.3. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

8.4. В целях внутреннего информационного обеспечения Учреждение может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, фотография, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

8.5. Доступ к обрабатываемым в Учреждении персональным данным разрешается только работникам, занимающим должности, включенные в перечень должностей структурных подразделений, при замещении которых осуществляется обработка персональных данных.

## 9. Перечень действий с персональными данными и способы их обработки

9.1. Учреждение осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление и уничтожение персональных данных.

9.2. Обработка персональных данных в Учреждении осуществляется 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.

## 10. Права субъектов персональных данных

Субъекты персональных данных имеют право на:

– полную информацию об их персональных данных, обрабатываемых в Учреждении;

– доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

– исключение или исправление неверных либо неполных персональных данных, а также данных, обрабатываемых с нарушением требований Трудового

кодекса Российской Федерации или иного федерального закона;

– уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

– дополнение своих персональных данных оценочного характера заявлением, выражающим их собственную точку зрения;

– извещение всех лиц, которым ранее были сообщены их неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– отзыв согласия на обработку персональных данных;

– принятие предусмотренных законом мер по защите своих прав;

– обжалование действия или бездействия Учреждения, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

– осуществление иных прав, предусмотренных законодательством Российской Федерации.

## 11. Меры, принимаемые для обеспечения выполнения обязанностей оператора при обработке персональных данных

11.1. Меры, необходимые и достаточные для обеспечения выполнения Учреждением обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

– назначение лица, ответственного за организацию обработки персональных данных;

– принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;

– организацию обучения и проведение методической работы с работниками структурных подразделений, занимающими должности, включенные в перечень должностей структурных подразделений, при замещении которых осуществляется обработка персональных данных;

– получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

– обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;

– обеспечение раздельного хранения персональных данных и их материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;

– организацию учета документов, содержащих персональные данные;

– установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны Учреждения и сети «Интернет» без применения установленных мер по обеспечению

безопасности персональных данных (за исключением общедоступных и (или) обезличенных персональных данных);

– обеспечение защиты документов, содержащих персональные данные, на бумажных и иных материальных носителях при их передаче третьим лицам с использованием услуг почтовой связи;

– хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;

– осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Учреждения;

– иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

11.2.Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с локальными нормативными актами Учреждения, регламентирующими вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Учреждения.

## 12. Контроль за соблюдением законодательства Российской Федерации и локальных нормативных актов ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России в области персональных данных, в том числе требований к защите персональных данных

12.1. Контроль за соблюдением структурными подразделениями Учреждения законодательства Российской Федерации и локальных нормативных актов Учреждения в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в структурных подразделениях законодательству Российской Федерации и локальным нормативным актам, в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

12.2. Внутренний контроль соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Учреждения осуществляет отдел информационной безопасности.

12.3. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов в области персональных данных в структурном подразделении, а также за обеспечение конфиденциальности и безопасности персональных данных возлагается на

руководителей структурных подразделений.

## 13. Порядок пересмотра Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России

Политика обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России пересматривается по мере необходимости. При пересмотре Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России учитываются результаты контроля эффективности обеспечения информационной безопасности за предыдущий период.

Процедура пересмотра Политики включает:

–анализ и выявление несоответствий действующей Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России текущим условиям;

–разработку предложений по совершенствованию Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России;

–утверждение новой редакции Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России.

При осуществлении процедуры пересмотра учитываются:

–результаты контроля состояния информационной безопасности и предложения структурных подразделений о совершенствовании процедур обеспечения информационной безопасности;

–изменения в организационно-штатной структуре ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России и в его информационной инфраструктуре;

–изменения в законодательной и нормативной базе по информационной безопасности, произошедшие с момента утверждения предыдущей Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России;

–результаты анализа происшедших инцидентов информационной безопасности, а также уязвимости и угрозы, выявленные в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России за время, прошедшее с момента утверждения предыдущей Политики обработки персональных данных в ФГБУ «НМИЦ онкологии им. Н.Н. Блохина» Минздрава России;

–изменения в управлении информационной безопасности, включая изменения в распределении ресурсов и обязанностей при обеспечении информационной безопасности.