

Политика конфиденциальности персональных данных в ФГБНУ «НИИГБ им. М.М. Краснова»

Настоящая Политика конфиденциальности персональных данных - (далее - Политика) действует в отношении всей информации, располагаемой ФГБНУ «НИИГБ им. М.М. Краснова», содержащей персональные данные.

1. Общие положения

1.1 Настоящая Политика разработана в соответствии с п. 2 ст. 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и является внутренним регулятивным документом ФГБНУ «НИИГБ им. М.М. Краснова» (далее – Организация, учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Организация.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в Организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Организацией как до, так и после утверждения Политики.

1.4. Обработка ПДн в Организации осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами, и определяемых: Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»; Федеральным законом "Об образовании в Российской Федерации" от 29.12.2012 N 273-ФЗ; Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»; Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; иными нормативными правовыми актами Российской Федерации. Кроме того, обработка ПДн в Организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Действующая редакция Политики хранится по месту нахождения Организации по адресу: г. Москва, ул. Россолимо, д.11, корп. А, электронная версия Политики - на сайте по адресу: niigb.ru

2. Термины и принятые сокращения

2.1 Персональные данные (ПДн) - любая информация, относящаяся к прямо или

косвенно определенному или определяемому физическому лицу (субъекту ПДн);

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 - 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;

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 (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Организация руководствуется следующими принципами:

3.2.1. Законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

3.2.2. Системность: обработка ПДн в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и

- факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
- 3.2.3. Комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- 3.2.4. Непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- 3.2.5. Своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- 3.2.6. Преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- 3.2.7. Персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- 3.2.8. Минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- 3.2.9. Гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования ИСПДн Организации, а также объема и состава обрабатываемых ПДн;
- 3.2.10. Специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- 3.2.11. Эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- 3.2.12. Наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- 3.2.13. Непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.
- 3.3. В Организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПДн уничтожаются или обезличиваются.
- 3.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.
4. Обработка персональных данных

4.1. Получение ПДн:

4.1.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПДн создаются путем:

копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.); внесения сведений в учетные формы; получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Организации.

4.2. Обработка ПДн:

4.2.1. Обработка персональных данных осуществляется: с согласия субъекта персональных данных на обработку его персональных данных; в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных 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 (далее - персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их трудовыми обязанностями и требованиями внутренних регулятивных документов Организации.

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

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

4.2.2. Цели обработки ПДн: обеспечение организации оказания медицинской помощи населению, научные исследования и разработки в области естественных и технических наук, подготовка кадров высшей квалификации, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011г № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 п № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации»; 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 РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование; представления

работодателем установленной законодательством отчетности в отношении физических лиц и отчетности работодателя, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ, сведений в Министерство науки и высшего образования Российской Федерации и иные организации.

4.2.3. Категории субъектов персональных данных

В Организации обрабатываются ПДн следующих субъектов: физические лица, состоящие с учреждением в трудовых отношениях; физические лица, являющиеся близкими родственниками сотрудников учреждения; физические лица, уволившиеся из учреждения; физические лица, являющиеся кандидатами на работу; физические лица, состоящие с учреждением в гражданско-правовых отношениях; физические лица, обратившиеся в учреждение за медицинской помощью, физические лица, обучающиеся по программам научно-педагогических кадров, по образовательным программам высшего образования, посетители проходящие в здании учреждения.

4.2.4. ПДн, обрабатываемые Организацией: данные, полученные при осуществлении трудовых отношений; данные, полученные для осуществления отбора кандидатов на работу в организацию; данные, полученные при осуществлении гражданско-правовых отношений; данные, полученные при оказании медицинской помощи, данные, полученные по обучению; данные, полученные для организации пропускного режима прохода в здание.

4.2.5. Обработка персональных данных ведется: с использованием средств автоматизации; без использования средств автоматизации.

4.3. Хранение ПДн:

4.3.1. ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.3. Не допускается хранение и размещение документов, содержащих ПДн, в открытых электронных каталогах (файлообменных сервисах).

4.3.4. Хранение ПДн в форме, позволяющей определить субъекта ПДн, 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.

4.4. Уничтожение ПДн:

4.4.1. Уничтожение документов (носителей), содержащих ПДн производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.4.2. ПДн на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

4.5. Передача ПДн

4.5.1. Организация передает ПДн третьим лицам в следующих случаях: субъект выразил свое согласие на такие действия; передача предусмотрена применимым законодательством

Российской Федерации в рамках установленной законодательством процедуры.

4.5.2. Перечень лиц, которым могут передаваться ПДн:

Третьи лица, которым могут передаваться ПДн: Обслуживающий работодателя банк (в рамках «зарплатного проекта»), иные банки для начисления заработной платы (на основании договора); отделения Пенсионного фонда РФ, Федеральной налоговой службы, Главное управление по вопросам миграции МВД России, Главное управление по контролю за оборотом наркотиков МВД России, отделения Фонда социального страхования РФ, Министерство науки и высшего образования РФ, Министерство здравоохранения РФ, Департамент труда и занятости населения, ГКУ Центр занятости населения (его отделения), Центральный объединенный архив, страховые (медицинские) организации, военные комиссариаты, руководители структурных подразделений работодателя, федеральный регистр медицинских, фармацевтических и педагогических работников, Фонд обязательного медицинского страхования (его территориальные органы); судебные и правоохранительные органы в случаях, установленных законодательством; бюро кредитных историй (с согласия субъекта).

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Организацией создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

5.5. Основными мерами защиты ПДн являются:

5.5.1. Введение должности в штатное расписание Организации и назначение лица ответственного за обработку ПДн, которое осуществляет организацию обработки ПДн, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПДн;

5.5.2. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД, и разработка мер и мероприятий по защите ПДн;

5.5.3. Разработка политики в отношении обработки персональных данных;

5.5.4. Установление правил доступа к ПДн, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПДн в ИСПД;

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями;

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПДн, обеспечение их сохранности;

5.5.7. Применение сертифицированного антивирусного программного обеспечения с

регулярно обновляемыми базами;

5.5.8. Применение сертифицированного программного средства защиты информации от несанкционированного доступа;

5.5.9. Применение сертифицированного межсетевое экрана и средств обнаружения вторжения;

5.5.10. Разработка и соблюдение условий, обеспечивающих сохранность ПДн и исключают несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн

5.5.11. Разработка и установление правил доступа к обрабатываемым ПДн, обеспечение регистрации и учета действий, совершаемых с ПДн, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер;

5.5.12. Восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

5.5.14. Организация и осуществление внутреннего контроля и аудита.

6. Основные права субъекта ПДн и обязанности Организации

6.1 Основные права субъекта ПДн

Субъект ПДн имеет право на получение информации, касающейся обработки его 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 Федеральным законом «О персональных данных»; информацию об осуществленной или о предполагаемой трансграничной передаче данных; наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Субъект ПДн 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, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Обязанности Организации

Организация обязана: при сборе ПДн предоставить информацию об обработке его ПДн; в случаях если ПДн были получены не от субъекта ПДн уведомить субъекта; при отказе в предоставлении ПДн субъекту разъясняются последствия такого отказа; опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПДн; принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн а также от иных неправомерных действий в отношении ПДн; давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

7. Ответственность

7.1. Организация, несет ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. В случае утраты или разглашения ПДн Организация не несёт ответственность, если данная конфиденциальная информация: стала публичным достоянием до её утраты или разглашения; была получена от третьей стороны до момента её получения Организацией; была разглашена с согласия Пользователя.

8. Разрешение споров

8.1. До обращения в суд с иском по спорам, возникающим из отношений между Пользователем и Организацией, обязательным является предъявление претензии (письменного предложения о добровольном урегулировании спора).

8.2. Получатель претензии в течение 30 календарных дней со дня ее получения, письменно уведомляет заявителя о результатах рассмотрения претензии.

8.3. При не достижении соглашения спор будет передан на рассмотрение в судебный орган в соответствии с действующим законодательством Российской Федерации.

8.4. К настоящей Политике конфиденциальности и отношениям между Пользователем и Организацией применяется действующее законодательство Российской Федерации.

9. Дополнительные условия

9.1. Организация имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента предусмотренного новой редакцией Политики. Организация вправе вносить изменения в настоящую Политику без согласия Пользователя.

Начальник отдела информационных технологий



А.В. Ситников