Приложение №1
к приказу № 251 от 14.08 2018г

Политика в области обработки и защиты персональных данных Федерального государственного бюджетного научного учреждения «Научно-исследовательский институт комплексных проблем сердечно-сосудистых заболеваний»

1. Общие положения

1.1. Федеральное государственное бюджетное научное учреждение «Научно-исследовательский институт комплексных проблем сердечно-сосудистых заболеваний» (далее Учреждение) является оператором персональных данных: Реестр операторов персональных данных – регистрационный номер 08-0021685.
В процессе осуществления уставной деятельности Учреждение обрабатывает персональные данные. Осуществляя обработку персональных данных (далее ПДн) Учреждение считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных.

1.2. Настоящая Политика обработки персональных данных в Учреждении (далее – Политика) определяет основные принципы, цели, условия и порядок обработки персональных данных, перечни субъектов и обрабатываемых в Учреждении персональных данных, функции Учреждения при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Учреждении требования к защите персональных данных.

1.3. Политика разработана с учетом требований Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 №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», законодательных и иных нормативных правовых актов Российской Федерации в области персональных данных.

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

1.5. Политика утверждается Директором Учреждения.

1.6. Политика распространяется на все случаи обработки персональных данных, вне зависимости от того, является обработка персональных данных автоматизированной или неавтоматизированной, производится она вручную или автоматически.

1.7. Политика является внутренним локальным нормативным актом Учреждения и является обязательной для исполнения всеми работниками.

1.8. Каждый работник, вновь принимаемый на работу в Учреждение, должен быть ознакомлен с Политикой под подпись.

1.9. Обработка персональных данных не может быть использована Учреждением или его работниками в целях причинения имущественного и морального вреда субъектам персональных данных, затруднения реализации их прав и свобод.

1.10. Обработка персональных данных в Учреждении должна ограничиваться достижением законных, конкретных и заранее определенных целей. Обработке подлежат только те персональные данные, и только в том объеме, которые отвечают целям их обработки.

1.11. Учреждение вправе вносить изменения в Политику по мере необходимости. Обязательный пересмотр Политики проводится в случае существенных изменений международного или национального законодательства в сфере персональных данных.

1.12. Политика является общедоступным документом. Для обеспечения неограниченного доступа к документу текст Политики размещается на общедоступном неопределенному кругу лиц сайте учреждения: kemcardio.ru.

2. Основные понятия

2.1. В Политике используются следующие основные понятия в соответствии с положением Закона №152-ФЗ:

персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемое с использованием средств автоматизации или без использования таких средств, 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 вычислительной техники;

информация – сведения (сообщения, данные) независимо от формы их представления;

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

оператор персональных данных (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;

субъект персональных данных – идентифицированное или не идентифицированное физическое лицо, в отношении которого проводится обработка персональных данных;

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;

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.

3. Цели и принципы обработки персональных данных

3.1. Учреждение, являясь оператором персональных данных, осуществляет обработку персональных данных исключительно в целях:

- осуществления возложенных на Учреждение Уставом и законодательством Российской Федерации функций;
- регулирования трудовых отношений с работниками (обеспечение социальной защиты и охраны здоровья, обучение и продвижение по службе, обеспечение личной безопасности, контроль количества и качества выполняемой работы) в соответствии с требованиями законодательства Российской Федерации;
- сохранение здоровья жителей, получение данных о заболеваемости, смертности, лечении, проведенных операциях;
- в иных законных целях.

3.2. Перечень персональных данных, обрабатываемых в Учреждении, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Учреждения с учетом целей обработки персональных данных.

3.3. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:

- законности и справедливой основы;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- 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.

3.4. Учреждение производит обработку ПДн при наличии хотя бы одного из следующих условий:

- обработка ПДн осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

- обработка ПДн необходима для осуществления и выполнения возложенных на Учреждение законодательством Российской Федерации функций, полномочий и обязанностей;

- обработка ПДн необходима для исполнения договоров, стороной которых является субъект персональных данных;

- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.4. Сроки обработки и хранения персональных данных определяются в соответствие со сроком действия договора с субъектом персональных данных, сроками хранения документов, установленными требованиями законодательства и нормативными документами, а также сроком предоставленного субъектом согласия на обработку персональных данных, в случаях, когда такое согласие должно быть предоставлено в соответствии с требованиями законодательства.

4. Перечень субъектов, персональные данные которых обрабатываются в Учреждении

4.1. В Учреждении обрабатываются персональные данные следующих категорий субъектов:

- работники Учреждения;
- пациенты Учреждения;
- партнеры и их представители;
- другие субъекты персональных данных (для обеспечения реализации целей обработки, указанных в разделе 3 Политики).

5. Категории персональных данных

5.1. В целях информированного обеспечения Учреждение может создавать общедоступные источники персональных данных субъектов, в том числе справочники и репортажи.

5.2. В общедоступные источники ПДн с письменного согласия субъекта могут включаться его фамилия, имя, отчество, дата рождения, должность, номера контактных телефонов, адрес электронной почты и иные персональные данные, сообщаемые субъектом ПДн.

5.3. Сведения о субъекте должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта либо по решению суда или иных уполномоченных государственных органов.

5.4. Обработка Учреждением специальных категорий ПДн, касающихся состояния здоровья, интимной жизни, расовой, национальной принадлежности, допускается в случаях, если:

- субъект ПДн дал согласие в письменной форме на обработку своих персональных данных;
- обработка ПДн осуществляется в соответствии с законодательством Российской Федерации;
- обработка ПДн необходима для защиты жизни, здоровья и иных жизненно важных интересов субъекта ПДн либо жизни, здоровья других лиц и получение согласия субъекта ПДн невозможно;
- обработка ПДн осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

6. Функции Учреждения при осуществлении обработки персональных данных

6.1. 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, а именно:

- 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 в Учреждении;
- осуществляет ознакомление работников Учреждения, 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;
- 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.

7. Условия обработки персональных данных в Учреждении

7.1. 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.

7.2. Учреждение без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

7.3. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора, если иное не предусмотрено федеральным законом. 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 «О персональных данных». Лицо, осуществляющее обработку ПДн по поручению оператора, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Законом №152-ФЗ.

7.4. 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, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.

7.5. Персональные данные в Учреждении могут обрабатываться только уполномоченными в установленном порядке работниками.

7.6. Работники допускаются в Учреждении к обработке персональных данных только приказом Директора.

7.7. Работники, допущенные к обработке персональных данных, имеют право приступать к работе с персональными данными только после ознакомления под личную роспись с локальными нормативными актами, регламентирующими обработку ПДн.

7.8. Работники, осуществляющие обработку персональных данных, должны действовать в соответствии с должностными инструкциями, регламентами и другими распорядительными документами Учреждения, и соблюдать требования Учреждения по соблюдению режима конфиденциальности.

8. Перечень действий с персональными данными и способы их обработки

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

8.2. 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.

8.3. Персональные данные хранятся исключительно на должным образом защищенных носителях, в том числе электронных.

8.4. Учреждение передает персональные данные третьим лицам, включая, но не ограничиваясь, Территориальный фонд обязательного медицинского страхования, страховые медицинские организации, партнеров, исполнителей по договорам, с вашего согласия для достижения указанных выше целей. Исключения составляют случаи, когда передача осуществляется для обеспечения соблюдения требований законодательства, предупреждения или пресечения ваших незаконных действий и защиты законных интересов Учреждения и третьих лиц.

9. Права и обязанности субъекта персональных данных

9.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

9.2. Обязанность подтвердить доказательство получения согласия субъекта ПДн на обработку его персональных данных или доказательство наличия оснований, указанных в Законе №152-ФЗ, возлагается на оператора.

9.3. Субъект персональных данных обязан предоставлять только достоверные и полные персональные данные, которые при необходимости должны быть документально подтверждены.

9.4. Субъект персональных данных имеет право на полную информацию, касающуюся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами.

9.5. Субъект персональных данных вправе получить доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом, а также на доступ к относящимся к нему медицинским данным с помощью медицинского специалиста.

9.6. Субъект персональных данных вправе требовать от Учреждения уточнения 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.

9.7. Субъект персональных данных вправе требовать от Учреждения отзыв согласия на обработку персональных данных, если такое право не ограничено в соответствии с федеральными законами;

9.8. Субъект персональных данных имеет право на 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 судебном порядке.

10. Меры по обеспечению безопасности ПДн при их обработке

10.1. До начала обработки персональных данных Учреждением предприняты правовые, технические и организационные меры необходимые и достаточные для

обеспечения выполнения обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных.

10.2. Обеспечение безопасности персональных данных достигается следующими способами:

- назначением должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- вводом в Учреждении режима конфиденциальности персональных данных, когда все документы и сведения, содержащие информацию о персональных данных, являются конфиденциальными;
- разработкой и утверждением локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
- определением типа угроз безопасности персональных данных, актуальных для информационных систем Учреждения с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных;
- утверждением перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- организацией режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.
- получением согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;
- использованием антивирусных средств и средств восстановления системы защиты ПДн;
- применением 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;
- применением в необходимых случаях средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации;
- установлением запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны и сетям Интернет без применения установленных в Учреждении мер по обеспечению безопасности персональных данных (за исключением общедоступных и (или) обезличенных персональных данных);
- выделением конкретных мест хранения персональных данных (материальных носителей) персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;
- установлением 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 данных;
- ознакомлением работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных сотрудников;

- запретом для работников, осуществляющих обработку персональных данных, проводить несанкционированное или нерегистрируемое копирование персональных данных, в том числе с использованием сменных носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото и видеосъемки;

- осуществлением внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам;

- осуществлением учета документов по обработке персональных данных без использования автоматизированных систем отдельным делопроизводством, хранением документов с отметкой «Персональные данные» в надежно запираемых помещениях, шкафах и сейфах, ключи от которых хранятся только у ответственных за данную деятельность работников;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- осуществлением внутреннего контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных в соответствии 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.

10.3. Внутренний контроль за соблюдением структурными подразделениями Учреждения законодательства Российской Федерации и локальных нормативных актов в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в структурных подразделениях, 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.

10.4. Внутренний контроль соответствия обработки персональных данных Закону №152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным нормативным актам Учреждения осуществляет отдел информационных технологий.

10.5. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных нормативных актов Учреждения в области персональных данных в структурных подразделениях Учреждения, а также за

обеспечение конфиденциальности и безопасности персональных данных в указанных подразделениях возлагается на их руководителей.

10.6. Каждый работник, получающий для работы документ, содержащий персональные данные, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

10.7. Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

10.8. Учреждение не несет ответственности за убытки и иные затраты, понесенные субъектами персональных данных в результате предоставления ими недостоверных и неполных персональных данных.

начальник ОИТ Шамина О.А.