**УТВЕРЖДАЮ**

Директор ФГБУЗ СОМЦ ФМБА России

_____ О.В. Стрельченко

«12» января 2017 г.

# ПОЛИТИКА
# В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

## 1. Общие положения

Политика в отношении обработки персональных данных (далее – Политика) разработана в соответствии с действующим законодательством Российской Федерации в области персональных данных и целями, задачами, принципами обеспечения безопасности персональных данных в ФГБУЗ СОМЦ ФМБА России (далее по тексту – Центр).

Целью Политики является обеспечение безопасности объектов защиты Центра от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Политика устанавливает ответственность руководства, а также определяет подход организации к управлению информационной безопасностью.

В Политике определены требования к работникам учреждения, степень их ответственности, структура и необходимый уровень защищенности информационных систем персональных данных и объектов информатизации, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в Центре.

Требования Политики распространяются на всех работников Центра.

Настоящая Политика определяет принципы, порядок и условия обработки персональных данных пациентов и работников учреждения, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также устанавливает ответственность должностных лиц учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

## 2. Основания и цели обработки персональных данных

Центр осуществляет обработку персональных данных в соответствии с Конституцией Российской Федерации, Федеральным законом от 21.11 2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», ст. ст. 85-90 Трудового кодекса Российской Федерации, «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными Постановлением Правительства Российской Федерации от 01.11.2012 № 1119, Постановлением Правительства Российской Федерации от21.03.2012 N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»,«Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15.09.2008 № 687.

Цели обработки персональных данных:

– обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12.04.2010 № 61-ФЗ «Об обращении лекарственных средств» и от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4.10.2012 № 1006;

– - осуществление трудовых отношений;

– - осуществление гражданско-правовых отношений.

В Центре обрабатываются следующие категории персональных данных:

– специальная категория персональных данных пациентов, касающаяся состояния здоровья;

– иные категории персональных данных работников оператора, позволяющих идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением специальной категории персональных данных в целях осуществления и выполнения, возложенных законодательством Российской Федерации, на оператора функций, полномочий и обязанностей по выполнение трудового законодательства, осуществления бухгалтерской и кадровой деятельности;

– общедоступные персональные данные работников оператора.

## 3. Принципы и условия обработки персональных данных

Обработка персональных данных Центре осуществляется на основе принципов:

– законности и справедливости целей и способов обработки персональных данных; соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

– хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки; уничтожения по достижении целей обработки персональных данных.

Обработка персональных данных пациентов осуществляется с письменного согласия субъекта персональных данных на обработку его персональных данных, а также если обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных.

Если получение согласия субъекта персональных данных невозможно, то обработка персональных данных осуществляется, только если она необходима для защиты жизни и здоровья или иных жизненно важных интересов субъекта персональных данных.

Обработка персональных данных работников осуществляется в соответствии с заключенным трудовым договором.

Доступ к обрабатываемым персональным данным, предоставляется только тем сотрудникам учреждения, которым он необходим в связи с исполнением ими своих должностных обязанностей и с соблюдением принципов персональной ответственности.

Прекращение неавтоматизированной обработки персональных данных пациентов и уничтожение документов, содержащих персональные данные, осуществляется по истечению сроков хранения.

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

Прекращение автоматизированной обработки персональных данных пациентов в информационных подсистемах персональных данных осуществляется:

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

– по истечению сроков хранения.

Прекращение автоматизированной и неавтоматизированной обработки персональных данных работников, осуществляется в следующих случаях:

– прекращение договорных отношений с работниками и физическими лицами;

– ликвидация учреждения.

Уничтожение документов, содержащих персональные данные работников, осуществляется по истечению сроков их хранения, которые регламентируются Федеральным законом от 06.12.2011 № 402-ФЗ «О бухгалтерском учете», Налоговым кодексом Российской Федерации, Перечнем типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения, утвержденным Министерством культуры и массовых коммуникаций Российской Федерации 31.07.2007 № 1182, «Перечнем документов со сроками хранения Министерства здравоохранения СССР, органов, учреждений, организаций, предприятий системы здравоохранения», введенным в действие Приказом Минздрава СССР от 30.05.1974 № 493.

Передача персональных данных третьим лицам осуществляется в следующих случаях если передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

Передача персональных данных третьим лицам осуществляется с использованием автоматизированных информационных систем по закрытым средствами криптографической защиты каналам связи и методом физической доставки адресату в распечатанном виде.

## 4. Обеспечение безопасности персональных данных

Важнейшим условием реализации целей деятельности Центра является обеспечение необходимого и достаточного уровня безопасности информационных систем персональных данных, соблюдения конфиденциальности, целостности и доступности обрабатываемых персональных данных и сохранности носителей сведений, содержащих персональные данные на всех этапах работы с ними.

Созданные в Центре условия и режим защиты информации, отнесенной к персональным данным, позволяет обеспечить защиту обрабатываемых персональных данных.

В Центре в соответствии с действующим законодательством Российской Федерации разработан и введен в действие комплекс организационно-распорядительных, функциональных и планирующих документов, регламентирующих и обеспечивающих безопасность обрабатываемых персональных данных.

Разработан перечень персональных данных, подлежащих защите. Выделены информационные системы персональных данных и проведена их классификация.

Для формирования обоснованных требований к обеспечению безопасности обрабатываемых персональных данных и проектирования системы защиты персональных данных разработаны частные модели угроз безопасности для каждой информационной системы персональных данных.

Определены перечни помещений, предназначенных для обработки и хранения персональных данных, перечень средств вычислительной техники, на которых разрешается обрабатывать персональные данные.

Введены режим безопасности обработки и обращения с персональными данными, а также режим защиты помещений, в которых осуществляется обработка и хранение носителей персональных данных;

Назначены ответственный за организацию и обеспечение безопасности персональных данных, администраторы информационных систем персональных данных и администратор безопасности информационных систем персональных данных, им определены обязанности и разработаны инструкции по обеспечению безопасности информации;

Определен круг лиц, имеющих право обработки персональных данных, разработаны инструкции пользователям по защите персональных данных, антивирусной защите, действиям в кризисных ситуациях;

Определены требования к персоналу, степень их ответственности, за обеспечение безопасности персональных данных.

Проведено ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации по обеспечению безопасности персональных данных и требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Проводится периодическое обучение указанных работников правилам обработки персональных данных.

Предприняты необходимые и достаточные технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий:

- введена система разграничения доступа;
- установлена защита от несанкционированного доступа к автоматизированным рабочим местам, информационным сетям и базам персональных данных;
- установлена защита от вредоносного программно-математического воздействия;
- осуществляется регулярное резервное копированием информации и баз данных;
- передача информации по сети общего пользования «Интернет» осуществляется с использованием средств криптографической защиты информации.

Организована система контроля за порядком обработки персональных данных и обеспечения их безопасности. Спланированы проверки соответствия системы защиты персональных данных, аудит уровня защищенности персональных данных в информационных системах персональных данных, функционирования средств защиты информации, выявления изменений в режиме обработки и защиты персональных данных.

## 5. Основные права субъекта персональных данных и Центра как оператора персональных данных

Права Центра:

– предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

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

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

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Центром;

– правовые основания и цели обработки персональных данных;

– цели и применяемые оператором способы обработки персональных данных;

– наименование и место нахождения Центра, сведения о лицах (за исключением Работников Центра), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Центром или на основании федерального закона;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных».

Субъект персональных данных вправе требовать от Центра 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. Заключительные положения

Настоящая Политика является общедоступной и подлежит размещению на официальном сайте или иным образом обеспечивается неограниченный доступ к данной Политике.

Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных Центра.

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

Ответственный за обеспечение информационной безопасности А.И. Фомченков