УТВЕРЖДЕНА
приказом ФГБУЗ ЮОМЦ ФМБА России
от «23» июня 2017 г. № 153

ПОЛИТИКА
Федерального государственного бюджетного учреждения здравоохранения «Южный окружной медицинский центр Федерального медико-биологического агентства» по обработке и защите персональных данных

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с п. 2 ст. 18.1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и является основополагающим внутренним регулятивным документом Федерального государственного бюджетного учреждения здравоохранения «Южный окружной медицинский центр Федерального медико-биологического агентства» (далее по тексту – Центр), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных, оператором которых является Центр.

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

1.3. В Политике применяются следующие сокращения, термины и определения:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

Дирекция – аппарат управления ФГБУЗ ЮОМЦ ФМБА России.

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

Лечащий врач – врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

Медицинская деятельность – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

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

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.

Пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

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

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

Работник – физическое лицо, вступившее в трудовые отношения с Центром.

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

Система защиты персональных данных (СЗПДн) – комплекс мер направленных на защиту персональных данных субъекта персональных данных.

Субъект персональных данных – человек, к которому относятся соответствующие персональные данные.

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.

Центр – ФГБУЗ ЮОМЦ ФМБА России (Дирекция и филиалы), являющийся оператором персональных данных.

1.4. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Центром как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.5. Обработка ПДн в Центре осуществляется в связи с выполнением функций, предусмотренных учредительными документами, и определяемых:

– Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– 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 Центре осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Центр выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией Центром своих прав и обязанностей как юридического лица.

1.6. Центр 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 ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.7. Действующая редакция хранится в месте нахождения Центра по адресу: Россия, Ростовская область, г. Ростов-на-Дону, ул. 1-я Линия, д.6, E-mail: uomc_fmba@uomc-mail.ru. Электронная версия Политики на сайте www.umedcentr.ru.

2. Принципы обеспечения безопасности персональных данных

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

2.2. Для обеспечения безопасности ПДн Центр руководствуется следующими принципами:

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

– системность: обработка ПДн в Центре осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

– комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Центра и других имеющихся в Центре систем и средств защиты;

– 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;

– своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

– преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в Центре с учетом выявления новых

способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

– персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

– минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

– гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных Центра, а также объема и состава обрабатываемых ПДн;

– специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

– эффективность процедур отбора кадров: кадровая политика Центра предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;

– 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;

– непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

2.3. В Центре не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в Центре, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Центром ПНд уничтожатся или обезличиваются.

2.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Центр принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Обработка персональных данных

3.1. Получение ПДн

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

3.1.2. Центр должен сообщить субъекту персональных данных 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 персональных данных дать письменное согласие на их получение.

3.1.3. Документы, содержащие ПДн создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и др.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и др.).

Порядок доступа субъекта персональных данных к его ПДн, обрабатываемым Центром, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Центра.

3.2. Обработка ПДн

3.2.1. 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 должностными обязанностями и требованиями внутренних документами Центра.

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

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

3.2.2. Цели обработки ПДн:

– обеспечение организации оказания медицинской помощи населению, 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 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;

– осуществление трудовых отношений;

– осуществление гражданско-правовых отношений.

3.2.3. Категории субъектов персональных данных

В Центре обрабатываются ПДн следующих субъектов персональных данных:

– физические лица, состоящие с Центром в трудовых отношениях;

– физические лица, являющие близкими родственниками Работников Центра;

– физические лица, уволившиеся из Центра;

– физические лица, являющиеся кандидатами на работу;

– физические лица, состоящие с Центром в гражданско-правовых отношениях;

– физические лица, обратившиеся в Центр за медицинской помощью.

3.2.4. ПДн, обрабатываемые Центром:

– данные полученные при осуществлении трудовых отношений;

– данные полученные для осуществления отбора кандидатов на работу в Центр;

– данные полученные при осуществлении гражданско-правовых отношений;

– данные полученные при оказании медицинской помощи.

3.2.5. Полный список конфиденциальной информации, в том числе и ПДн для Дирекции утверждается директором Центра, для филиалов главным врачом филиала.

3.2.6. Обработка персональных данных ведется:

– с использованием средств автоматизации.

– без использования средств автоматизации.

3.3. Хранение ПДн

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

3.3.2. ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах, либо в запираемых помещениях с ограниченным правом доступа.

3.3.3. ПДн субъектов персональных данных, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных ИСПДн.

3.3.4. Не допускается хранение и размещение документов, содержащих ПДн, в открытых информационных ресурсах (электронных каталогах, файлообменниках, файловых хранилищах, на общедоступных сайтах и т.п.).

3.3.5. Хранение ПДн 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.

3.4. Уничтожение ПДн

3.4.1. 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.

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

3.4.3. ПДн в ИСПДн уничтожаются путем удаления записей субъекта персональных данных.

3.4.4. Уничтожение производится комиссией по информационной безопасности. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

3.5. Передача ПДн

3.5.1. Центр передает ПДн третьим лицам в следующих случаях:

– Субъект персональных данных выразил свое согласие на такие действия;

– передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

3.5.2. Перечень лиц, которым передаются ПДн

Третьи лица, которым передаются ПДн:

– Федеральное медико-биологическое агентство;

– Пенсионный фонд РФ для учета (на законных основаниях);

– Налоговые органы РФ (на законных основаниях);

– Фонд социального страхования (на законных основаниях);

– Территориальный фонд обязательного медицинского страхования (на законных основаниях);

– страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);

– банки для начисления заработной платы (на основании договора);

– судебные и правоохранительные органы в случаях, установленных законодательством;

– бюро кредитных историй (с согласия субъекта персональных данных);

– юридические фирмы, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта персональных данных).

4. Защита персональных данных

4.1. В соответствии с требованиями нормативных документов Центром создана система защиты персональных данных (СЗПДн), состоящая из подсистем правовой, организационной и технической защиты.

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

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

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

4.5. Основными мерами защиты ПДн, используемыми Центром, являются:

4.5.1. Назначение лица ответственного за организацию обработки и обеспечения безопасности ПДн;

4.5.2. Назначение администратора информационной безопасности ИСПДн, который осуществляет обучение и инструктаж, внутренний контроль над соблюдением Центром и его Работниками требований к защите ПДн;

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

4.5.4. Разработка политики в отношении обработки персональных данных;

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

4.5.6. Установление индивидуальных паролей доступа Работников Центра в информационную систему в соответствии с их производственными обязанностями;

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

4.5.8. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами;

4.5.9. Сертифицированное программное средство защиты информации от несанкционированного доступа;

4.5.10. Сертифицированные межсетевой экран и средство обнаружения вторжения;

4.5.11. Соблюдение условий, обеспечивающих сохранность ПДн и исключающие несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн

4.5.12. 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;

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

4.5.14. Инструктаж Работников, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику Центра в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

4.5.15. Осуществление внутреннего контроля и аудита.

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

5.1. Основные права субъекта персональных данных

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;

– 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 Центра, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

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.

5.2. Обязанности Центра

Центр обязан:

– при сборе ПДн предоставить информацию об обработке персональных данных субъекта персональных данных;

– при отказе в предоставлении ПДн субъекту персональных данных 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 персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных.