УТВЕРЖДАЮ
Директор
ФГБУЗ ЗСМЦ ФМБА России
_____ /В.Ю. Шутов/
«28» 09 20 16 г.

ПОЛОЖЕНИЕ
об обработке, передаче и защите персональных данных работников и пациентов ФГБУЗ ЗСМЦ ФМБА России

1. Общие положения

Настоящее «Положение об обработке и защите персональных данных работников и пациентов ФГБУЗ ЗСМЦ ФМБА России» (далее по тексту - «Положение») устанавливает порядок приема, учета, сбора, поиска, обработки, накопления, хранения и передачи документов, содержащих сведения, отнесенные действующим законодательством Российской Федерации к персональным данным сотрудников и пациентов Федерального государственного бюджетного учреждения здравоохранения «Западно-Сибирский медицинский центр Федерального медико-биологического агентства» (далее по тексту: «ФГБУЗ ЗСМЦ ФМБА России», «Учреждение», «Центр»). При этом под сотрудниками Центра подразумеваются физические лица, имеющие с Центром трудовые отношения. Под пациентами подразумеваются физические лица, которым Центр оказывает либо намеревается оказать медицинские услуги в соответствии с лицензией на право осуществления медицинской деятельности, выданной Учреждению.

1.1. Цель

Настоящее Положение является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся в Учреждении как у работодателя и исполнителя оказания медицинских услуг населению, посредством планомерных действий по совершенствованию организации труда в Учреждении.

1.2. Основания

Основанием для разработки данного Положения являются:

- Конституция РФ от 12.12.1993г.;
- Трудовой кодекс РФ № 197-ФЗ от 01.02.2002г.;
- Кодекс РФ об административных правонарушениях № 195-ФЗ от 30.12.2001г.;
- Федеральный закон от 20.02.1995г. № 24-ФЗ «Об информации, информатизации и защите информации»;
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"
- Указ Президента РФ от 06.09.1997г. №188 «Об утверждении перечня сведений конфиденциального характера»;
- Федеральный закон от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации"
- Устав ФГБУЗ ЗСМЦ ФМБА России.

1.3. Порядок ввода в действие Положения о защите персональных данных и изменений к нему

Настоящее Положение и изменения к нему вводятся в действие приказом по Учреждению и утверждаются директором Центра. Все сотрудники Учреждения, имеющие

доступ к персональным данным сотрудников/пациентов, должны быть ознакомлены с данным Положением и изменениями к нему под расписку.

2. Понятие и состав персональных данных

2.1. Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией. К персональным данным сотрудников Центра относятся:

- все биографические сведения сотрудника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- номера домашнего и мобильных телефонов;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкеты сотрудников;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным сотрудника.

2.2. Под персональными данными пациентов Центра понимается информация, ставшая известной сотрудникам Центра в связи с оказанием пациентам консультационных, амбулаторно-поликлинических и стационарных медицинских услуг в связи с добровольным обращением пациента за оказанием медицинской помощи того или иного вида, касающаяся конкретного пациента, а также сведения о фактах, событиях и обстоятельствах жизни пациента, позволяющих идентифицировать его личность. К персональным данным пациентов Центра относятся:

- все биографические сведения пациента;
- образование;
- специальность;
- занимаемая должность;
- адрес местожительства;
- номера домашнего и мобильных телефонов;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- факт обращения пациента в Центр за оказанием медицинской помощи;
- информация о состоянии здоровья и диагнозе пациента;

- данные, содержащиеся в амбулаторной карте пациента, либо в медицинской карте стационарного больного, в иной медицинской документации;
- иные сведения, полученные при медицинском обследовании и лечении пациента (врачебная тайна).

Указанные данные и документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.3. Собственником информационных ресурсов (персональных данных) является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем; либо вступил с Центром в отношения по оказанию медицинских услуг. Субъект персональных данных самостоятельно решает вопрос передачи Учреждению своих персональных данных.

2.4. Держателем персональных данных является Учреждение (работодатель/исполнитель услуг), которому сотрудник или пациент добровольно передает во владение свои персональные данные. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

2.5. Права и обязанности Учреждения как работодателя в трудовых отношениях и как исполнителя услуг в отношениях Центр-пациент осуществляются физическим лицом, уполномоченным Учреждением. Указанные права и обязанности директор Центра может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников/пациентов или связана с обработкой этих данных.

2.6. Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

3.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. Получение, хранение, комбинирование, передача или любое другое использование персональных данных пациента также осуществляются в целях обеспечения соблюдения законодательства в сфере здравоохранения, наиболее эффективной реализации прав и интересов пациента при оказании медицинской помощи, обеспечения личной безопасности пациента, контроля своевременности и качества оказании медицинских услуг.

3.4. Все персональные данные сотрудника/пациента получаются у него самого. Если персональные данные сотрудника/пациента возможно получить только у третьей стороны, то сотрудник/пациент должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Учреждение должно сообщить сотруднику/пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

3.5. Не допускается получение и обработка персональных данных сотрудника/пациента о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

3.6. При принятии решений относительно сотрудника/пациента на основании его персональных данных, не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ, возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

3.7. Пакет анкетно-биографических и характеризующих материалов (далее - «пакет») сотрудника формируется после издания приказа о его приеме на работу. Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу.

Все документы хранятся в папках в алфавитном порядке фамилий сотрудников.

Пакет пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

3.8. Сотрудник отдела кадровой и правовой работы Центра, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

3.9. Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

3.10. При обработке персональных данных сотрудников работодатель в лице директора Центра вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников Центра на базе современных информационных технологий.

3.11. Сотрудник Центра обязан:

– передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;

– своевременно сообщать работодателю об изменении своих персональных данных.

3.12. Сотрудник/пациент имеет право на:

– полную информацию о своих персональных данных и обработке этих данных;

– свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника/пациента, за исключением случаев, предусмотренных законодательством РФ;

– определение своих представителей для защиты своих персональных данных;

– доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;

– требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе Учреждения исключить или исправить персональные данные сотрудника/пациента, он имеет право заявить в письменной форме о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требование об извещении Центром всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника/пациента, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжалование в суд любых неправомерных действий или бездействия Учреждения при обработке и защите его персональных данных.

4. Доступ к персональным данным

4.1. Персональные данные добровольно передаются сотрудником/пациентом непосредственно держателю этих данных и потребителям внутри Учреждения исключительно для обработки и использования в работе.

4.2. Внешний доступ.

К числу массовых потребителей персональных данных вне Учреждения можно отнести следующие государственные и негосударственные функциональные структуры:

- подразделения муниципальных органов управления;
- военкоматы;
- налоговые инспекции;
- судебные органы;
- правоохранительные органы;
- органы исполнения наказаний;
- органы статистики;
- медицинские страховые компании;
- органы социального и медицинского страхования;
- пенсионные и иные внебюджетные фонды;
- банки;
- органы государственного казначейства.

4.3. Внутренний доступ.

Внутри Учреждения к разряду потребителей персональных данных работников/пациентов Центра относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- директор Центра;
- заместитель директора по терапии;
- заместитель директора по хирургии;
- заместитель директора по организационно-методической работе;
- начальник и сотрудники отдела оказания высокотехнологичной медицинской помощи (ВМП);
- начальник и сотрудники отдела кадровой и правовой работы;
- начальник и сотрудники отдела автоматизированных систем управления (АСУ);
- начальник и сотрудники отдела внебюджетной деятельности;
- начальник и сотрудники финансово-экономической службы;
- начальник и сотрудники организационно-методического отдела;
- главный бухгалтер и сотрудники бухгалтерии;
- начальник и сотрудники канцелярии;
- сотрудники регистратуры поликлиники;
- заведующий, врачи и средний медицинский персонал поликлиники;
- заведующий, врачи и средний медицинский персонал детской поликлиники;
- заведующий, врачи и средний медицинский персонал дневного стационара;
- заведующие отделениями, врачи и средний медицинский персонал стационара;
- сотрудники Консультативного Диагностического Центра (КДЦ);
- заведующий и сотрудники клинико-диагностической лаборатории (КДЛ).
- заведующий, врачи и средний медицинский персонал стоматологической поликлиники.

4.4. В отделе кадровой и правовой работы Центра хранятся личные карточки сотрудников, как работающих в настоящее время, так и работавших в Центре ранее. Для этого используются специально оборудованные шкафы или сейфы, которые запираются на ключ. Личные карточки располагаются в алфавитном порядке.

После увольнения документы по личному составу передаются на хранение в архив Учреждения (предельный срок хранения личных дел сотрудников установлен действующим законодательством РФ).

5. Передача персональных данных

5.1. При передаче персональных данных сотрудника/пациента работодатель должен соблюдать следующие требования:

5.1.1. Передача внешнему потребителю:

– передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;

– при передаче персональных данных сотрудника/пациента потребителям (в том числе и в коммерческих целях) за пределы Центра, последний не должен сообщать эти данные третьей стороне без письменного согласия сотрудника/пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника/пациента или в случаях, прямо установленных федеральным законом;

– ответы на правомерные письменные запросы коммерческих фирм, учреждений и организаций даются с разрешения директора Центра и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;

– не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;

– по возможности персональные данные обезличиваются.

5.1.2. Передача внутреннему потребителю.

Центр вправе разрешать доступ к персональным данным сотрудников/пациентов Центра другим сотрудникам Учреждения только в целях служебной необходимости. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников и пациентов Центра (Приложение №1).

6. Защита персональных данных

6.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

6.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

6.3. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и хозяйственной деятельности Учреждения.

6.4. Внутренняя защита.

6.4.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал Учреждения, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам

данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Центра.

6.4.2. Для защиты персональных данных сотрудников/пациентов Центра необходимо соблюдать ряд взаимосвязанных мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно–методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- запрет выдачи личных дел сотрудников на рабочие места руководителей подразделений. Личные дела могут выдаваться только на рабочее место директора Центра, и в исключительных случаях, по письменному разрешению директора, руководителю структурного подразделения;
- защита персональных компьютеров, в которых содержатся персональные данные сотрудников/пациентов Центра, соответствующими паролями доступа;
- определение из числа сотрудников Центра лица, ответственного за защиту персональных данных, и наделение его соответствующими полномочиями.

6.5. Внешняя защита.

6.5.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и завладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

6.5.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадровой и правовой работы, а также в отделе АСУ.

6.5.3. Для защиты персональных данных сотрудников/пациентов необходимо соблюдать ряд взаимосвязанных мер:

- порядок приема, учета и контроля деятельности посетителей Центра;
- пропускной режим Центра;
- порядок охраны территории, зданий, помещений, транспортных средств Учреждения;
- внутренний порядок согласования предоставления той или иной конфиденциальной информации третьим лицам;
- порядок электронного обмена информацией сотрудников Центра между собой и с третьими лицами;

— порядок передачи информации третьим лицам на бумажных носителях.

6. Лицо, ответственное за защиту конфиденциальной информации, связанной с персональными данными

6.1. Лицом, ответственным за защиту персональных данных сотрудников/пациентов Центра, является Ведущий специалист по защите информации, состоящий в штате отдела автоматизированных систем управления (АСУ) отдела организационно-методической работы ФГБУЗ ЗСМЦ ФМБА России.

6.2. Ведущий специалист по защите информации назначается на должность приказом по Учреждению и действует на основании должностной инструкции, утверждаемой директором Центра.

6.3. Ведущий специалист по защите информации выполняет работы (включая особо сложные) по комплексной защите информации в Учреждении, обеспечивая эффективное применение всех имеющихся организационных и инженерно-технических мер в целях защиты сведений, содержащих персональные данные сотрудников/пациентов Центра.

6.4. В рамках своих должностных обязанностей Ведущий специалист по защите информации вправе контролировать соблюдение норм действующего законодательства РФ в сфере защиты персональных данных, а также требований настоящего Положения всеми сотрудниками Центра, имеющими доступ к персональным данным работников/пациентов Центра, включая руководителей структурных подразделений (список таких сотрудников указан в Приложении №2 к настоящему Положению).

6.5. Лица, имеющие доступ к персональным данным, в свою очередь, обязаны всемерно содействовать Ведущему специалисту по защите информации в осуществлении им своих должностных обязанностей, в том числе, немедленно сообщать о любых ставших им известными случаях (попытках) несанкционированного доступа третьих лиц к информации, содержащей персональные данные.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

7.2. Руководитель, разрешающий доступ сотрудника Центра к тому или иному конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.3. Каждый сотрудник Учреждения, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность письменного или электронного носителя и за конфиденциальность ставшей ему известной информации.

7.4. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, *административную, гражданско–правовую или уголовную ответственность граждан и* юридических лиц.