

Приложение №1 к приказу ОГБУЗ «ТЦМК»
От «29» 08 2018г. № 44а

ПОЛОЖЕНИЕ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
областного государственного бюджетного учреждения здравоохранения
«ТЕРРИТОРИАЛЬНЫЙ ЦЕНТР МЕДИЦИНЫ КАТАСТРОФ»

1. Общие положения.

1.1. Настоящее Положение разработано в целях защиты персональных данных, обрабатываемых в информационных системах персональных данных Областного государственного казенного учреждения здравоохранения «Территориальный центр медицины катастроф» (далее ОГБУЗ «ТЦМК»), от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Положение определяет обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты Персональных данных, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

1.3. Положение разработано на основании ст. 24 Конституции РФ, Федерального закона РФ «О персональных данных» № 152-ФЗ от 27.07.2006 г., Закона «Об информации, информатизации и защите информации» № 149-ФЗ от 27.07.2006 г., Постановления Правительства Российской Федерации от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативно-правовыми актами Российской Федерации в области трудовых отношений.

1.4. Настоящее Положение утверждается руководителем ОГБУЗ «ТЦМК».

1.5. Изменения в Положение могут быть внесены в установленном действующим законодательством порядке.

1.6. В настоящем Положении используются следующие основные понятия:

1.6.1. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) – работнику, абитуриенту, обучающемуся, выпускнику;

1.6.2 Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

1.6.3. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

1.6.4. Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-

телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

1.6.5. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

1.6.6. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

1.6.7. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

1.6.8. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

1.6.9. Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

1.6.10. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

1.6.11. Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

1.6.12. Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2. Понятие и содержание персональных данных.

2.1. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в частности, в ОГБУЗ «ТЦМК» – информация, необходимая для осуществления основной деятельности ОГБУЗ «ТЦМК» и кадрового учета сотрудников.

2.2. Оператором персональных данных является ОГБУЗ «ТЦМК».

2.3. Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений.

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

2.5. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания и в отношении общедоступных персональных данных.

3. Порядок обработки персональных данных.

3.1. Обработка персональных данных Субъектов осуществляется в следующих целях:

- выполнения возложенных на оператора функций, полномочий и обязанностей;
- соблюдения законов и иных нормативных правовых актов, в том числе в целях реализации прав Субъектов персональных данных;
- содействия Субъектам персональных данных в трудоустройстве, обучении и повышении в должности;
- в иных целях, предусмотренных действующим законодательством.

3.2. Обработка персональных данных Субъектов должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Оператора;
- 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 ИСПДн;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных.

3.3. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативными-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Оператора.

3.4. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальной и расовой принадлежности, политических и религиозных убеждениях.

3.5. Не допускается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

3.6. Правила обработки и использования персональных данных устанавливаются отдельными нормативными правовыми и распорядительными актами Оператора.

3.7. Персональные данные могут храниться в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативных правовых актов Российской Федерации мер по защите персональных данных.

3.8. Перечень структурных подразделений и (или) отдельных должностей, имеющих право на обработку персональных данных определяются отдельными Приказами, распорядительными документами и иными письменными указаниями уполномоченных сотрудников Оператора.

3.9. Обеспечения конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных Субъекта;
- в отношении общедоступных персональных данных Субъектов, которые создаются в целях информационного обеспечения деятельности Оператора (в том числе справочники, адресные книги). В общедоступные источники персональных данных Субъектов с письменного согласия Субъекта могут включаться его фамилия, имя, отчество, год и место рождения, адрес и иные персональные данные, предоставленные Субъектом.

Сведения о Субъекте могут быть в любое время исключены из общедоступных источников персональных данных по требованию Субъекта либо по решению суда или иных уполномоченных государственных органов.

3.10. Оператор осуществляет обработку персональных данных Субъекта как в автоматизированной, так и в неавтоматизированной форме. Особенности способов обработки персональных данных (автоматизированная/неавтоматизированная) и защиты персональных данных могут быть установлены правовыми актами Оператора в соответствии с требованиями, предусмотренными действующим законодательством.

3.11. При передаче персональных данных Оператор не вправе:

- сообщать персональные данные Субъекта третьей стороне без письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в других случаях, предусмотренных Федеральными законами;
- сообщать персональные данные Субъекта в коммерческих целях без его письменного согласия.

3.12. При передаче персональных данных Оператор обязан:

- предупредить лиц, получающих персональные данные Субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные Субъекта, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными Субъектов в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным Субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные Субъекта, которые необходимы для выполнения конкретных функций;
- выполнять иные обязанности, предусмотренные федеральными законами и настоящим Положением.

Персональные данные Субъекта могут быть переданы представителям Субъектов в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

3.13. В случае достижения цели обработки персональных данных Субъектов Оператор обязан незамедлительно прекратить обработку персональных данных Субъекта и уничтожить соответствующие персональные данные в срок, предусмотренный законодательством Российской Федерации.

3.14. Иные требования к обработке персональных данных Субъекта определяются действующим трудовым законодательством и законодательством о защите персональных данных.

3.1. Особенности обработки персональных данных в ИСПДн с использованием средств автоматизации

3.1.1. Информационные системы, предназначенные для обработки персональных данных, должны быть приведены в соответствие с требованиями действующего законодательства Российской Федерации, нормативных распорядительных актов и рекомендаций регулирующих органов в области защиты информации, нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

3.1.2. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации ИСПДн;
- настроенных программных и технических средств защиты в соответствии с требованиями безопасности информации;
- охраной и пожарной сигнализацией и организации режима допуска в

помещения, предназначенные для обработки персональных данных.

3.1.3. Пользователь информационной системы персональных данных обязан соблюдать правила и технологию обработки информации, отраженную в Инструкции пользователя ИСПДн.

3.2. Особенности обработки персональных данных в ИСПДн без использования средств автоматизации

3.2.1. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

3.2.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

3.2.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

3.2.4. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

3.2.5. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

3.2.6. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

3.2.7. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же

носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

3.2.8. Должны быть созданы надлежащие условия, обеспечивающие сохранность документов и внешних электронных носителей информации, содержащих персональные данные.

3.2.9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных

4.1. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

4.1.1. На получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;

4.1.2. Требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

4.1.3. На получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;

4.1.4. На обжалование действий или бездействия Оператора в

уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

4.1.5. На защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.2. Обязанности Оператора при сборе персональных данных:

4.2.1. Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

4.2.2. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

4.2.3. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения.

4.2.4. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные.

4.2.5. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.

4.2.6. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных и законодательством Российской Федерации.

4.2.7. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных.

4.3. Права Оператора на передачу персональных данных третьим лицам.

4.3.1. Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

5. Доступ к персональным данным субъекта

5.1. Доступ к персональным данным Субъекта ограничивается в соответствии с федеральными законами и настоящим Положением.

5.2. Доступ к персональным данным Субъектов имеют только сотрудники Оператора, утвержденные руководителем ОГБУЗ «ТЦМК» для каждой из ИСПДн.

5.3. Разрешительная система допуска лиц (должностей), в обязанности которых входит обработка персональных данных или которые по должности имеют доступ к персональным данным с правом просмотра, разрабатывается ответственным за обеспечение безопасности персональных данных при их обработке в ИСПДн.

5.4. Представители Оператора имеют право получать только те персональные данные Субъекта, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц и утвержденной системой допуска. Все остальные работники Оператора, являющиеся Субъектами персональных данных, имеют право на полную информацию только о своих персональных данных.

6. Меры по защите персональных данных субъекта

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

6.2. Оператор определяет перечень своих Представителей, имеющих право доступа и обработки информации о персональных данных, и соответствующие уровни доступа к этой информации.

6.3. Оператор утверждает формы ведения учета выданных персональных данных (если соответствующие формы не определены действующим законодательством) и уполномочивает своих Представителей на их ведение.

6.4. При автоматизированной обработке персональных данных Оператор использует специальное программное обеспечение и аппаратные средства, соответствующие предусмотренным действующим законодательством требованиям.

6.5. Оператор в предусмотренном Трудовым кодексом Российской Федерации порядке проводит ознакомление Субъектов, являющихся работниками Оператора, с нормативными правовыми актами в области защиты персональных данных, в том числе в случае их изменения, разъясняет права, обязанности и ответственность Субъектов за нарушение норм в данной области.

6.6. Оператор устанавливает особый режим хранения для документов, содержащих персональные данные Субъектов. Персональные данные Субъектов, содержащиеся на бумажных носителях, должны храниться в запираемом шкафу или в сейфе.

6.7. Ключи от кабинетов уполномоченных Представителей сдаются при выходе из здания под охрану.

6.8. Доступ к персональным данным Субъекта, содержащимся в ИСПДн, ограничивается определенными Оператором сотрудниками.

6.9. Сроки хранения документов устанавливаются Оператором в соответствии с требованиями действующего законодательства.

7. Ответственность за разглашение конфиденциальной информации, содержащей персональные данные субъектов

7.1. Оператор, а также должностные лица, виновные в нарушении требований действующего законодательства, правовых актов, регулирующих обработку и защиту персональных данных Субъекта, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном законодательством Российской Федерации ответственность.

7.2. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные.