государственное бюджетное учреждение здравоохранения
Ставропольского края «Левокумская центральная районная больница»

П Р И К А З

03 ноября 2015 г. с. Левокумское № 131

Об утверждении положения об организации работы с персональными данными в государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница»

В соответствии с главой 14 ТК РФ, Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", от 01 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных"

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемое Положение об организации работы с персональными данными в государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница» (далее – Положение).
2. Работникам ГБУЗ СК «Левокумская ЦРБ» в своей работе руководствоваться Положением.
3. Признать утратившим силу приказ главного врача ГБУЗ СК «Левокумская ЦРБ» от 31.01.2013 года № 16 «Об утверждении Положения о хранении и использовании персональных данных работников».
4. Программисту ГБУЗ СК «Левокумская ЦРБ» Салогубову В.А. разместить Положение на официальном сайте ГБУЗ СК «Левокумская ЦРБ».
5. Специалисту по кадрам ГБУЗ СК «Левокумская ЦРБ» Алексенко И.И. ознакомить под роспись работников ГБУЗ СК «Левокумская ЦРБ» с настоящим приказом и Положением.
6. Настоящий приказ вступает в силу со дня его подписания.

Главный врач
ГБУЗ СК «Левокумская ЦРБ» Е.И. Девяткина

УТВЕРЖДЕНО
приказом главного врача
ГБУЗ СК «Левокумская ЦРБ»
от 03.11.2015 г. № 131

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ ЗДРАВООХРАНЕНИЯ СТАВРОПОЛЬСКОГО КРАЯ «ЛЕВОКУМСКАЯ ЦЕНТРАЛЬНАЯ РАЙОННАЯ БОЛЬНИЦА»

1. Общие положения

1.1. Настоящее Положение об организации работы с персональными данными в государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница» (далее - Положение) устанавливает правила обработки персональных данных в государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница», процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяет для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3. Действие настоящего Положения не распространяется на отношения, возникающие при:

1) обработке персональных данных, отнесенных к сведениям, составляющим государственную тайну;

2) организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской

Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

1.4. Понятия, используемые в настоящем Положении, применяются в значениях, определенных Федеральными законами.

1.5. К категориям субъектов персональных данных, обрабатываемых в государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница», относятся:

1) лица, состоящие в трудовых отношениях с государственным бюджетным учреждением здравоохранения Ставропольского края «Левокумская центральная районная больница»;

2) лица, состоящие в иных гражданско-правовых отношениях с государственным бюджетным учреждением здравоохранения Ставропольского края «Левокумская центральная районная больница»;

3) лица, претендующие на замещение должностей в государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница» и на включение в кадровый резерв;

4) физические лица, обратившиеся в государственное бюджетное учреждение здравоохранения Ставропольского края «Левокумская центральная районная больница» с жалобами, заявлениями и по другим вопросам;

5) физические лица, обратившиеся в государственное бюджетное учреждение здравоохранения Ставропольского края «Левокумская центральная районная больница» за предоставлением государственных (муниципальных) услуг, оказываемых государственным бюджетным учреждением здравоохранения Ставропольского края «Левокумская центральная районная больница»;

6) физические лица, обратившиеся в государственное бюджетное учреждение здравоохранения Ставропольского края «Левокумская центральная районная больница» с целью получения медицинских услуг, либо состоящие в иных гражданско-правовых отношениях с Учреждением по вопросам получения медицинских услуг.

2. Цели обработки персональных данных

2.1. В государственном бюджетном учреждении здравоохранения Ставропольского края «Левокумская центральная районная больница» (далее – Учреждение) обработка персональных данных осуществляется в следующих целях:

1) осуществление возложенных на Учреждение, как оператора, обрабатывающего персональные данные, полномочий в соответствии с законодательством Российской Федерации и законодательством Ставропольского края;

2) организация учета лиц, состоящих в трудовых отношениях

(работники) и иных гражданско-правовых отношениях с Учреждением для обеспечения соблюдения законодательства Российской Федерации и законодательства Ставропольского края в сфере трудовых отношений и пенсионного обеспечения;

3) предоставление и обеспечение предоставления государственных (муниципальных) услуг в соответствии с Федеральным законом «Об организации предоставления государственных и муниципальных услуг»;

4) заполнение базы данных автоматизированной информационной системы персональных данных Учреждения в целях повышения эффективности работы и быстрого поиска, проведения мониторинговых исследований, формирования статистических и аналитических отчетов.

2.2. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.3. При обработке персональных данных не допускается:

1) объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

2) обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Порядок сбора и уточнения персональных данных

3.1. Субъект персональных данных представляет свои персональные данные при заключении трудового договора и в иных случаях, установленных законодательством Российской Федерации и законодательством Ставропольского края.

3.2. Сбор в Учреждении документов, содержащих персональные данные, осуществляется путем их приобщения к материалам личных дел субъектов персональных данных либо путем создания, в том числе копирования представленных оригиналов документов, внесения сведений в учетные формы (на бумажных и электронных носителях).

3.3. Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

Уточнение персональных данных производится только на основании полученной в соответствии с законодательством Российской Федерации порядке информации.

3.4. Субъект персональных данных представляет свои персональные данные самостоятельно либо через своего представителя. В случаях, предусмотренных законодательством Российской Федерации, персональные данные также могут быть переданы Учреждению третьими лицами.

3.5. Обработка персональных данных осуществляется с согласия

субъекта персональных данных на их обработку, составленного в письменном виде по форме, утверждаемой Учреждением. Согласие на обработку персональных данных подписывается субъектом персональных данных собственноручно либо его представителем. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного электронной подписью в соответствии с Федеральным законом «Об электронной подписи».

В случае если согласие на обработку персональных данных дается представителем субъекта персональных данных от лица субъекта персональных данных, Учреждение проверяет полномочия представителя.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в порядке, предусмотренном законодательством Российской Федерации.

3.6. При получении персональных данных от субъекта персональных данных или его представителя Учреждение:

1) разъясняет права, цели и порядок обработки персональных данных;

2) предлагает представить согласие на обработку персональных данных по форме, утверждаемой Учреждением;

3) разъясняет последствия отказа предоставить персональные данные, передача которых в соответствии с законодательством Российской Федерации является обязательной.

3.7. Лица, состоящие в трудовых отношениях (работники) с Учреждением, лица, состоящие в иных гражданско-правовых отношениях с Учреждением, осуществляющие обработку, хранение, передачу и обезличивание персональных данных (далее - Уполномоченные лица) при получении персональных данных от субъекта персональных данных подписывают обязательство о соблюдении конфиденциальности персональных данных, а в случае расторжения с ними трудовых договоров - о прекращении обработки персональных данных, ставших известными им в связи с исполнением должностных обязанностей.

4. Правила обработки персональных данных

4.1. Уполномоченные лица, осуществляющие обработку, хранение, передачу и обезличивание персональных данных, обязаны:

1) знать и выполнять требования законодательства Российской Федерации в области обеспечения защиты персональных данных, а также настоящего Положения;

2) хранить в тайне известные им персональные данные, информировать о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним;

3) соблюдать правила использования персональных данных, порядок их учета и хранения, исключить доступ к ним посторонних лиц;

4) обрабатывать только те персональные данные, к которым получен доступ в силу исполнения должностных обязанностей.

4.2. При обработке персональных данных уполномоченным лицам запрещается:

1) использовать сведения, содержащие персональные данные, в неслужебных целях, а также в служебных целях - при ведении переговоров по телефонной сети, в открытой переписке, статьях и выступлениях;

2) передавать персональные данные по незащищенным каналам связи (телетайп, факсимильная связь, электронная почта) без использования сертифицированных средств криптографической защиты информации;

3) снимать копии с документов и других носителей информации, содержащих персональные данные, или производить выписки из них, а равно использовать различные технические средства (видео- и звукозаписывающую аппаратуру) для фиксации сведений, содержащих персональные данные;

4) выполнять за пределами Учреждения работы, связанные с использованием персональных данных, выносить документы и другие носители информации, содержащие персональные данные, из Учреждения.

4.3. Уполномоченные лица, виновные в нарушении требований законодательства Российской Федерации о защите персональных данных, в том числе допустившие разглашение персональных данных, - несут персональную гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

4.4. Процедурами, направленными на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, являются:

1) назначение ответственных лиц за организацию обработки персональных данных;

2) определение уполномоченных лиц, несущих ответственность в соответствии с законодательством Российской Федерации за нарушение защиты персональных данных;

3) ознакомление уполномоченных лиц с положениями законодательства Российской Федерации в области обеспечения защиты персональных данных и настоящим Положением;

4) определение лиц, ответственных за обеспечение безопасности информационных систем персональных данных Учреждения;

5) получение у субъекта персональных данных согласия на обработку его персональных данных;

6) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

7) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации и настоящего Положения;

8) размещение на официальном сайте Учреждения в информационно-телекоммуникационной сети «Интернет» правовых актов Учреждения в сфере персональных данных (далее - акты Учреждения), ознакомление уполномоченных лиц с актами Учреждения;

9) запрет на обработку персональных данных лицами, не допущенными к их обработке;

10) ограничение на обработку персональных данных под диктовку;

11) осуществление внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации о защите персональных данных.

4.5. Обработка персональных данных в Учреждении осуществляется в информационных системах персональных данных Учреждения с использованием средств автоматизации и без использования средств автоматизации.

4.6. Обработка персональных данных в информационных системах персональных данных Учреждения с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», другими нормативными правовыми актами Российской Федерации.

4.7. При эксплуатации автоматизированных информационных систем необходимо соблюдать следующие требования:

1) к работе в автоматизированных информационных системах допускаются только уполномоченные лица и лица ответственные за организацию обработки персональных данных;

2) на персональных электронных вычислительных машинах (далее - ПЭВМ), дисках, папках и файлах, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);

3) на период обработки персональных данных в помещении могут находиться только уполномоченные лица и лица ответственные за организацию обработки персональных данных;

4) допуск других лиц в указанный период может осуществляться с разрешения Руководителя Учреждения или лица, ответственного за обеспечение безопасности персональных данных в Учреждении.

4.8. Персональные данные, которые обрабатываются в информационных системах Учреждения, подлежат защите от несанкционированного доступа и копирования.

Безопасность персональных данных при их обработке в информационных системах персональных данных Учреждения обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства

предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять требованиям, обеспечивающим защиту информации, устанавливаемым законодательством Российской Федерации.

4.9. Реализация требований по обеспечению безопасности персональных данных в информационных системах персональных данных Учреждения возлагается на ведущего программиста и программиста Учреждения совместно со структурными подразделениями Учреждения, эксплуатирующими эти системы.

При обработке персональных данных субъектов персональных данных в информационных системах персональных данных Учреждения ведущим программистом и программистом Учреждения совместно с лицами, состоящие в трудовых отношениях с Учреждением и лицами, состоящими в иных гражданско-правовых отношениях с Учреждением, эксплуатирующими эти системы, обеспечивается:

1) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

3) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

5) постоянный контроль за обеспечением уровня защищенности персональных данных.

4.10. Защита персональных данных при их обработке в информационных системах персональных данных осуществляется в соответствии с Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.11. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и путем применения программных и технических средств.

4.12. Самостоятельное подключение ПЭВМ, применяемых в Учреждении для обработки, хранения или передачи персональных данных, к информационно-телекоммуникационным сетям (в том числе к информационно-телекоммуникационной сети «Интернет»), позволяющим

осуществлять передачу персональных данных через государственную границу Российской Федерации, не допускается.

4.13. Доступ уполномоченных лиц к персональным данным в информационных системах персональных данных Учреждения разрешается после обязательного прохождения процедур идентификации и аутентификации.

4.14. Уполномоченными лицами при обработке персональных данных в информационных системах персональных данных Учреждения должно обеспечиваться:

1) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства Учреждения;

2) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

3) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4) постоянный контроль за обеспечением уровня защищенности персональных данных;

5) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

6) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

7) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

8) в случае выявления нарушений порядка обработки персональных данных в информационных системах Учреждения принятие мер по установлению причин нарушений и их устранению;

9) разбирательство и составление заключений по фактам несоблюдения условий хранения бумажных и электронных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

4.15. Руководители структурных подразделений Учреждения, работники структурных подразделений Учреждения (далее соответственно - руководители структурных подразделений, работники), осуществляющие обработку персональных данных, обязаны контролировать и выполнять предусмотренные в Учреждении меры по защите информации, содержащей

персональные данные.

4.16. Руководители структурных подразделений обязаны:

1) участвовать в подготовке перечня персональных данных, обрабатываемых на ПЭВМ этих структурных подразделений;

2) готовить к утверждению списки работников, которых по своим должностным обязанностям необходимо допустить к работе с персональными данными в информационной системе Учреждения;

3) контролировать · целевое использование работниками ресурсов информационно-телекоммуникационной сети "Интернет";

4) контролировать выполнение пользователями общих правил работы на ПЭВМ, в локальной вычислительной сети Учреждения (далее - ЛВС), в информационных системах Учреждения;

5) контролировать выборочно характер исходящей информации, направляемой пользователями по электронной почте другим адресатам, и принимать оперативные меры к соблюдению ими установленных требований по защите персональных данных;

6) обеспечивать условия для работы комиссии Учреждения по контролю защищенности персональных данных при проверке в структурных подразделениях Учреждения эффективности предусмотренных мер защиты информации;

7) определять порядок передачи информации, содержащей персональные данные, другим структурным подразделениям Учреждения, сторонним организациям и иным органам;

8) при обнаружении нарушений установленных требований по защите персональных данных, в результате которых вскрыты факты их разглашения, прекратить работы на рабочем месте, где обнаружены нарушения, доложить руководителю Учреждения и поставить в известность лицо, ответственное за обеспечение безопасности персональных данных в Учреждении.

4.17. Работник обязан:

1) знать правила работы в ЛВС, информационных системах Учреждения и принятые меры по защите их ресурсов (в части, его касающейся);

2) выполнять только служебные задания, при работе на своей рабочей станции (ПЭВМ), в ЛВС и информационных системах Учрежедния;

3) проверить перед началом работы на ПЭВМ свои рабочие папки на жестком диске, съемные носители информации на отсутствие вирусов с помощью штатных средств антивирусной защиты, убедиться в исправности своей рабочей станции;

4) прекратить работу при сообщениях тестовых программ о появлении вирусов, доложить администратору по обеспечению безопасности информационных систем в Учреждении;

5) провести проверку носителей, при необходимости их использования, поступивших из других структурных подразделений Учреждения, на отсутствие вирусов;

6) хранить в тайне свой индивидуальный пароль для входа на свою рабочую станцию (ПЭВМ) и информационную систему, в которой производится обработка персональных данных, периодически, но не реже чем один раз в полгода изменять данный индивидуальный пароль для входа на рабочую станцию (ПЭВМ) и не сообщать его другим лицам;

7) вводить пароль для входа на свою рабочую станцию (ПЭВМ) и в информационные системы, в которых производится обработка персональных данных, и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

8) учет, размножение, обращение печатных материалов, содержащих персональные данные, проводить в соответствии с Инструкцией по делопроизводству;

9) при обнаружении различных неисправностей в работе компьютерной техники или ЛВС, недокументированных свойств в программном обеспечении, нарушений целостности пломб (наклеек, печатей), несоответствии номеров на аппаратных средствах сообщить об этом ответственному за обработку персональных данных в Учреждении и поставить в известность руководителя структурного подразделения.

4.18. Работнику при работе на своей рабочей станции (ПЭВМ) запрещается:

1) приносить различные компьютерные программы и пытаться установить их на локальный диск ПЭВМ без уведомления ответственного за обработку персональных данных в Учреждении;

2) перенастраивать программное обеспечение ПЭВМ;

3) самостоятельно вскрывать комплектующие рабочей станции (ПЭВМ);

4) запускать на своей рабочей станции (ПЭВМ) или другой рабочей станции сети любые системные или прикладные программы, кроме установленных ответственным за обработку персональных данных в Учреждении;

5) изменять или копировать файл, принадлежащий другому пользователю, не получив предварительно разрешения владельца файла;

6) оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

7) оставлять без личного присмотра свое персональное устройство идентификации (при наличии), электронные носители и документы, содержащие персональные данные;

8) допускать к подключенной в сеть рабочей станции (ПЭВМ) посторонних лиц;

9) производить копирование для временного хранения информации, содержащей персональные данные, на неучтенные носители;

10) работать на рабочей станции (ПЭВМ) в сети с информацией, содержащей персональные данные, при обнаружении неисправностей

станции (ПЭВМ), влияющих на защиту информации;

11) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к утечке, блокированию, искажению или утере информации, содержащей персональные данные;

12) отсылать по электронной почте информацию для решения личных проблем, а также информацию по просьбе третьих лиц без согласования с руководителем структурного подразделения;

13) запрашивать и получать из информационно-телекоммуникационной сети "Интернет" материалы развлекательного характера (игры, клипы и т.д.).

4.19. Работники не могут использовать в личных целях персональные данные, ставшие известными им вследствие выполнения должностных обязанностей.

4.20. 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 банных) на электронных носителях информации.

4.21. Персональные данные субъектов персональных данных при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

4.22. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4.23. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4.24. Документы, содержащие персональные данные, формируются уполномоченными лицами 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.

4.25. Использование персональных данных осуществляется с момента их получения уполномоченным лицом и прекращается:

1) по достижении целей обработки персональных данных;

2) в связи с отсутствием необходимости в достижении заранее заявленных целей обработки персональных данных.

4.26. Обработка персональных данных на бумажных носителях осуществляется уполномоченными лицами в соответствии с Инструкцией по

ведению делопроизводства.

4.27. В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

4.28. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

5. Порядок хранения и уничтожения персональных данных

5.1. Бумажные и электронные носители, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.2. Сроки обработки и хранения персональных данных определяются:

1) приказом Минкультуры Российской Федерации от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием

сроков хранения»;

2) сроком исковой давности;

3) иными требованиями законодательства Российской Федерации, нормативными правовыми актами Ставропольского края и внутренними документами Учреждения.

5.3. Базы данных информационных систем персональных данных Учреждения хранятся в структурных подразделениях Учреждения, осуществляющих их эксплуатацию, в соответствии со сроками хранения документов, помещенных в базы данных.

5.4. Уничтожение обработанных персональных данных производится путем сожжения, расплавления, дробления, растворения, химического разложения или превращения в мягкую бесформенную массу или порошок. Допускается уничтожение бумажных носителей путем измельчения в бумажную сечку. Электронные носители уничтожаются путем сожжения, дробления, расплавления и другими способами, исключающими возможность их восстановления.

5.5. Уничтожение бумажных и электронных носителей, содержащих персональные данные, осуществляется комиссией и оформляется актом об уничтожении.

Состав комиссии утверждается Учреждением.

5.6. Уничтожение бумажных и электронных носителей, содержащих персональные данные, без оформления акта об уничтожении запрещается.

Без оформления акта об уничтожении уничтожаются испорченные бумажные и электронные носители, черновики и проекты документов, и другие материалы, образовавшиеся при исполнении документов, содержащих персональные данные.

В процедуру уничтожения документов и носителей информации без составления акта об уничтожении документов входит проведение следующих мероприятий:

1) разрывание листов, разрушение носителя в присутствии исполнителя и руководителя структурного подразделения, допущенных к обработке персональных данных;

2) физическое уничтожение остатков носителей несколькими работниками, допущенными к работе с персональными данными.

5.7. Уничтожение или обезличивание части персональных данных, если это допускается бумажным или электронным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на данном носителе (удаление, вымарывание).

6. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

6.1. В Учреждении внутренний контроль соответствия обработки персональных данных установленным требованиям осуществляется путем проведения плановых и внеплановых проверок условий обработки персональных данных (далее - проверка) на основании плана осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, определяющего цель и срок проведения проверки, утвержденного Учреждением.

6.2. Проверка осуществляется ответственным за организацию обработки персональных данных в Учреждении либо комиссией по контролю соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении, состав которой утверждается руководителем Учреждения (далее - комиссия).

Количественный состав комиссии не должен быть менее трех работников Учреждения.

В проведении проверки не может участвовать работник Учреждения, прямо или косвенно заинтересованный в ее результатах.

6.3. Плановые проверки проводятся не чаще чем один раз в год.

6.4. В случае поступившего в Учреждение письменного заявления субъекта персональных данных о нарушениях правил обработки персональных данных проводится внеплановая проверка. Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления соответствующего заявления.

6.5. При проведении проверки соответствия обработки персональных данных установленным требованиям к защите персональных данных должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

2) порядок и условия применения средств защиты информации;

3) эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных Учреждения;

4) состояние учета машинных носителей персональных данных;

5) соблюдение правил доступа к персональным данным;

6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

7) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) осуществление мероприятий по обеспечению целостности персональных данных.

6.6. Лицо, ответственное за организацию обработки персональных

данных в Учреждении, и комиссия при проведении внутреннего контроля имеют право:

1) запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;

2) вносить главному врачу Учреждения (далее - главный врач) следующие предложения:

- по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

- о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

6.7. В ходе проведения внутреннего контроля лицо, ответственное за организацию обработки персональных данных в Учреждении, и комиссия должны обеспечивать конфиденциальность персональных данных.

6.8. Проверка должна быть завершена не позднее чем через 20 календарных дней со дня принятия решения о ее проведении.

6.9. По результатам проверки, проведенной комиссией, непосредственно после ее завершения составляется акт, который подписывается всеми членами комиссии. Председатель комиссии по результатам проверки представляет главному врачу письменное заключение о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений.

В случае проведения проверки лицом, ответственным за организацию обработки персональных данных в учреждении, непосредственно после ее завершения им составляется и подписывается акт. Лицо, ответственное за организацию обработки персональных данных в Учреждении, по результатам проверки представляет главному врачу письменное заключение о результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений.

7. Правила работы с обезличенными персональными данными

7.1. Под обезличиванием персональных данных в настоящем Положении понимаются действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

7.2. Обезличивание персональных данных может быть проведено в целях уменьшения ущерба от разглашения персональных данных, снижения класса информационных систем персональных данных Учреждения, по достижении целей обработки или в случае утраты необходимости в

достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

7.3. В Учреждении обезличивание персональных данных при условии их дальнейшей обработки осуществляется следующими способами:

1) сокращение перечня обрабатываемых персональных данных;

2) замена части сведений идентификаторами;

3) понижение точности некоторых сведений в зависимости от цели обработки персональных данных;

4) обработка разных персональных данных в разных информационных системах персональных данных Учреждения.

7.4. Ответственность за обезличивание персональных данных несут работники Учреждения, ответственные за проведение мероприятий по обезличиванию обрабатываемых персональных данных.

Перечень указанных лиц утверждается руководителем Учреждения.

7.5. Руководители структурных подразделений Учреждения, в которых осуществляется обработка персональных данных, вносят лицу, ответственному за организацию обработки персональных данных в Учреждении, предложения по обезличиванию персональных данных с указанием обоснования обезличивания персональных данных и способа их обезличивания.

7.6. Уполномоченные лица в случае согласования лица, ответственного за организацию обработки персональных данных в Учреждении, с обезличиванием персональных данных осуществляют его разрешенным способом.

7.7. Обезличенные персональные данные конфиденциальны и не подлежат разглашению.

7.8. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

7.9. При обработке обезличенных персональных данных с использованием средств автоматизации уполномоченные лица обязаны соблюдать парольную и антивирусную политику, правила работы со съемными носителями (если он используется), правила резервного копирования, порядок доступа в помещения, в которых ведется обработка персональных данных.

7.10. При обработке обезличенных персональных данных без использования средств автоматизации уполномоченные лица обязаны соблюдать правила хранения бумажных носителей и порядок доступа в помещения, в которых ведется обработка персональных данных.

8. Порядок доступа работников Учреждения в помещения, в которых ведется обработка персональных данных

8.1. Помещения, в которых ведется обработка персональных данных (далее - помещения), должны обеспечивать сохранность информации и

технических средств, исключать возможность бесконтрольного проникновения в помещения и их визуального просмотра посторонними лицами.

Помещения запираются на ключ и в случаях предусмотренных требованиями законодательства Российской Федерации опечатываются. Ключи от помещений хранятся у уполномоченных лиц Учреждения.

8.2. Персональные данные на бумажных и электронных носителях должны находиться шкафах, сейфах или на стеллажах, полках в закрытых папках (скоросшивателях).

8.3. Вскрытие и закрытие (опечатывание) помещений осуществляется уполномоченными лицами.

8.4. Перед закрытием (опечатыванием) помещения по окончании работы уполномоченные лица обязаны:

1) убрать бумажные и электронные носители, содержащие персональные данные в шкафы (сейфы) или на стеллажи, полки в закрыты папки (скоросшиватели);

2) отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

3) закрыть окна;

4) закрыть двери помещения;

8.5. Перед открытием помещения уполномоченные лица обязаны:

1) провести внешний осмотр двери и дверного замка с целью установления их целостности;

2) открыть дверь и осмотреть помещение, проверить наличие и целостность замка на сейфе.

8.6. При обнаружении факта взлома двери и (или) дверного замка помещения уполномоченные лица обязаны:

1) не вскрывая помещение, незамедлительно сообщить непосредственному руководителю;

2) в присутствии не менее двух уполномоченных лиц и непосредственного руководителя вскрыть помещение и осмотреть его;

3) составить акт о факте взлома двери и (или) дверного замка и передать его лицу, ответственному за организацию обработки персональных данных в Учреждении.

8.7. На время работы с персональными данными двери в помещения должны быть всегда закрыты.

Уборка помещений и проведение в них ремонтных работ осуществляются в присутствии уполномоченных лиц.

8.8. В случае необходимости принятия в выходные или нерабочие праздничные дни экстренных мер при авариях в системах энерго-, водо- и теплоснабжения помещения вскрываются уполномоченным лицом и руководителем соответствующего структурного подразделения.

8.9. Уполномоченным лицам запрещается передавать ключи от помещений третьим лицам.

8.10. Ответственность за соблюдение порядка доступа в помещения возлагается на руководителей структурных подразделений, в которых ведется обработка персональных данных.

Главный врач
ГБУЗ СК «Левокумская ЦРБ» Е.И. Девяткина