

ПРИКАЗ № 153

с. Большая Соснова

25.11.2024г.

**Об утверждении Положения о защите, хранении, обработке и передаче персональных данных работников и пациентов**

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных), Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", и иными нормативными правовыми актами в области обработки и защиты персональных данных,

**ПРИКАЗЫВАЮ:**

1. Утвердить:
  - 1.1. Положение о защите, хранении, обработке и передаче персональных данных работников и пациентов ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» (приложение 1).
2. Утвердить список лиц, допущенных к обработке персональных данных работников и пациентов с использованием средств автоматизации и без использования этих средств ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.»:
  - Главный врач;
  - заместитель главного врача;
  - сотрудник отдела кадров, в пределах своей компетенции;
  - сотрудники бухгалтерии и экономист, в пределах своей компетенции;Руководители структурных подразделений учреждения (только относительно работников своего подразделения);
  - Врачи и средний медицинский персонал-обработка персональных данных пациентов.
3. Внешний доступ персональных данных работников и пациентов может осуществляться только по запросу компетентных органов, имеющих соответствующие полномочия.
4. Ответственным лицам ознакомить всех сотрудников по своим подразделениям с Положением по обработке и защите персональных данных работников и пациентов и заключить с ними обязательство о неразглашении персональных данных.
5. Признать приказ ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» № 76 от 19.04.2021 г. «Об утверждении положения о защите персональных данных», утратившим силу.
6. Разместить приказ № 153 от 25.11.2024г. «Об утверждении Положения по обработке и защите персональных данных работников и пациентов» на официальном сайте «бснбол.рф».
7. Приказ вступает в силу с момента подписания.
8. Ответственность за исполнением приказа – персональная.

Главный врач  
ГБУЗ ПК «Большесосновская ЦРБ  
им. Колчановой Г.Ф.»



С.А. Рубцова

**Положение  
о защите, хранении, обработке и передаче персональных данных работников и  
пациентов ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.»**

**1. Общие положения**

- 1.1. Настоящее положение регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных), Приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", и иными нормативными правовыми актами в области обработки и защиты персональных данных.
- 1.2. Персональные данные работника - информация, необходимая ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.», (далее - медицинская организация, работодатель) в связи с трудовыми отношениями и касающаяся конкретного работника. Персональные данные пациента - информация, полученная медицинской организацией при первоначальном поступлении пациента, при заключении с пациентом договора на оказание медицинских услуг, а также информация, полученная в процессе оказания медицинской помощи.
- 1.3. Целью настоящего Положения является защита персональных данных Работников и Пациентов от несанкционированного доступа и разглашения, обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных в Государственном бюджетном учреждении здравоохранения Пермского края «Большесосновская центральная районная больница им. Колчановой Галины Федоровны» (далее - ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.»), в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Персональные данные являются конфиденциальной, строго охраняемой информацией.
- 1.4. Положение определяет: цель обработки персональных данных; категории субъектов, персональные данные которых обрабатываются; категории обрабатываемых персональных данных; правовое основание обработки персональных данных; перечень действий с персональными данными, способы и порядок обработки персональных данных; условие прекращения обработки персональных данных; реализуемые меры защиты и обеспечения безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации; обязанности лиц, непосредственно осуществляющих обработку персональных данных, и лица, ответственного за организацию обработки персональных данных; ответственность за нарушение требований законодательства Российской Федерации о персональных данных.
- 1.4. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» является оператором персональных данных (юридическим лицом) и зарегистрировано в реестре операторов, осуществляющих обработку персональных данных.

1.5. При обработке персональных данных, ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» руководствуется требованиями законодательства Российской Федерации в области персональных данных.

1.6. Настоящим Положением обязаны руководствоваться все лица, непосредственно осуществляющие обработку персональных данных, либо получившие доступ к персональным данным в ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.».

## **II. Категории субъектов, персональные данные которых обрабатываются**

2.1. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» обрабатывает персональные данные, принадлежащие следующим категориям субъектов персональных данных:

- работникам, состоящим с ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» в трудовых отношениях;

- пациентам ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.».

2.2. К персональным данным работника относятся:

- фамилия, имя, отчество;
- пол;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- сведения об образовании, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ медицинского образования, о документах об образовании и (или) о квалификации, о договоре о целевом обучении, а также данные о сертификате специалиста или о прохождении аккредитации специалиста;
- наименование организации, осуществляющей медицинскую деятельность;
- занимаемая должность в организации, осуществляющей медицинскую деятельность;
- сведения о членстве в медицинских профессиональных некоммерческих организациях;
- иные сведения, необходимые работодателю в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

2.3. К персональным данным пациента относятся:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- номер полиса обязательного медицинского страхования застрахованного лица;
- анамнез;
- диагноз;
- сведения об организации, осуществляющей медицинскую деятельность;
- вид оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;

- объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах;
- результат обращения за медицинской помощью;
- серия и номер выданного листка нетрудоспособности;
- сведения о проведенных медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты;
- примененные клинические рекомендации;
- сведения о медицинском работнике или медицинских работниках, оказавших медицинскую помощь, проводивших медицинские экспертизы, медицинские осмотры и медицинские освидетельствования;
- иные сведения, необходимые медицинской организации в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

### **III. Перечень действий с персональными данными, способы обработки персональных данных**

- 3.1. С персональными данными работников и пациентов совершаются следующее действие (операция) или совокупность действий (операций): сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, передача (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
- 3.2. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» обрабатывает персональные данные смешанным способом (с использованием средств автоматизации и без использования таких средств) с передачей персональных данных по локальной сети.
- 3.3. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» не поручает обработку персональных данных другим лицам.
- 3.4. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» не осуществляет трансграничную передачу персональных данных.
- 3.5. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» осуществляет раскрытие персональных данных врачей и среднего медицинского персонала (фамилия, имя, отчество, уровень образования и квалификации) неопределенному кругу лиц путем размещения указанных данных на сайте РИАМС ПРОМЕД- ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» в соответствии с требованием Федерального Закона «Об основах охраны здоровья граждан в Российской Федерации» № 323-ФЗ от 21.11.2011г.

### **IV. Реализуемые меры защиты и обеспечения безопасности персональных данных**

- 4.1. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» при обработке персональных данных реализует правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

### **V. Обязанности лиц, непосредственно осуществляющих обработку персональных данных**

- 5.1. Работники ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.», непосредственно осуществляющие обработку персональных данных, обязаны знать положения законодательства Российской Федерации о персональных данных, в том числе требования к защите персональных данных, документы, определяющие политику ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» в отношении обработки персональных данных, локальные акты ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» по вопросам обработки персональных данных.
- 5.2. Работники ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.», получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не

распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

5.3. В случае попытки третьих лиц получить от работника информацию, содержащую персональные данные, работник обязан незамедлительно сообщать об этом непосредственному руководителю.

5.4. Работник не использует информацию, содержащую персональные данные, с целью получения выгоды.

## VI. Обязанности лица, ответственного за организацию обработки персональных данных

6.1. Лицо, ответственное за организацию обработки персональных данных в ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» назначается приказом главного врача ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.».

6.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от главного врача ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» и подотчетно ему.

6.3. Лицо, ответственное за организацию обработки персональных данных в ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» обязано:

-осуществлять внутренний контроль за соблюдением в ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» и непосредственно его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

-доводить до сведения работников ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

-осуществлять прием и обработку обращений и запросов субъектов персональных данных или их представителей.

-информировать персонал информационной системы о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации информационной системы;

-доводить до персонала информационной системы требования по защите информации, а также положения организационно-распорядительных документов по защите информации, разработанные в учреждении с учетом внесенных в них изменений;

-обучать персонал информационной системы правилам эксплуатации отдельных средств защиты информации;

-проводить практические занятия и тренировки с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты;

-осуществлять контроль осведомленности персонала информационной системы об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

Практические занятия и тренировки с персоналом, мероприятия по обучению персонала и контролю осведомленности персонала устанавливаются оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в два года.

6.4. Распространение персональных данных-действия, направленные на раскрытие персональных данных определенному кругу лиц;

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

- 6.6. Блокирование персональных данных- временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных);
- 6.7. Уничтожение персональных данных-действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников;
- 6.8. Обезличивание персональных данных-действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту (работнику);
- 6.9. Информационная система персональных данных- система, представляющая совокупность содержащихся в базах персональных данных и обеспечивающих обработку их информационных технологий и технических средств;
- 6.10. Конфиденциальность персональных данных- обязательное для соблюдения назначенными ответственными лицами требование.
- Сотрудники Больницы, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.
- 6.11. Общедоступные персональные данные- персональные данные, доступ неограниченного круга лиц которым предоставлены с согласия субъекта персональных данных или на которых в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
- Обеспечение конфиденциальности не требуется:
- в случае обезличивания персональных данных;
  - в отношении общедоступных персональных данных.

## **VII. Обязанности Больницы**

- 7.1. Обработка персональных данных Пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.
- 7.2. При определении объема и содержания обрабатываемых персональных данных Пациентов Больница должна руководствоваться Конституцией Российской Федерации, ФЗ «о персональных данных» и иными федеральными законами.
- 7.3. Больница при Обработке персональных данных принимает необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
- Защита персональных данных Пациента от неправомерного их использования или утраты должна обеспечиваться больницей за счет собственных средств.

## **VIII. Сбор, обработка и хранение персональных данных.**

- 8.1. всю информацию о персональных данных Пациент предоставляет самостоятельно. Если персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его здоровья или иных жизненно важных интересов либо жизни, здоровья, прав и законных интересов других лиц, и получения согласия субъекта персональных данных невозможно;
- 8.2. Больница должна сообщить Пациенту о последствиях отказа Пациента дать согласие на их получение.
- Перечень оснований для приостановления или отказа в предоставлении услуги:
- отсутствие документов, которые Пациент должен предоставить для получения услуги (полис, паспорт);
  - нарушение Пациентом общепринятых норм поведения (оскорбления сотрудников, пациентов больницы, неадекватное поведение, алкогольное или токсическое опьянение и др.).

Медицинская помощь по экстренным показаниям может быть предоставлена без предъявления документов. Отсутствие документов у пациента не может являться причиной отказа в экстренной медицинской помощи.

В случае отказа Пациента предоставить персональные данные или их неполного предоставления, Больница при необходимости не вправе выписать листок нетрудоспособности (больничный лист), при необходимости включить в Реестр по выдаче льготных лекарств, направить на обследование, медицинские комиссии, выписать направления на анализы и т.д.

8.3. Пациент предоставляет больнице достоверные сведения о себе.

### **IX. Передача персональных данных**

9.1. Выдача персональных данных самому пациенту происходит с отметкой в журнале учета носителей, содержащих персональные данные и с подписью самого пациента о получении этого документа.

9.2. При передаче персональных данных Пациента третьим лицам Больница должна соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия пациента за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

- лица, получающие персональные данные Пациента, обязаны соблюдать конфиденциальность;

- разрешать доступ к персональным данным Пациента только специально уполномоченым лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

9.3. Не допускается разглашение сведений, составляющих врачебную тайну лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме оговоренных законов случаев.

Так предоставление сведения, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

- в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

- по запросу органов дознания и следствия и суда в связи с проведением расследования или судебным разбирательством;

- в случае оказания помощи несовершеннолетнему в возрасте, установленном частью 24 «Основ законодательства», для информирования его родителей или законных представителей;

- при наличии оснований, позволяющих полагать, что вред здоровью гражданина причинен в результате противоправных действий;

- в целях проведения военно-врачебной экспертизы в порядке, установленном Положением о военно-врачебной экспертизе, утверждаемым уполномоченным федеральным органом исполнительной власти.

### **X. Обеспечение защиты информации**

10.1. Обеспечение защиты информации в ходе эксплуатации информационной системы должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать следующие мероприятия:

планирование мероприятий по защите информации в информационной системе;

анализ угроз безопасности информации в информационной системе;

управление (администрирование) системой защиты информации информационной системы;

управление конфигурацией информационной системы и ее системой защиты информации;  
реагирование на инциденты;  
информирование и обучение персонала информационной системы;  
контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе.

10.2. Сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных частями 3 и 4 статьи 13 Федерального закона от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации".

10.3. Все персональные сведения о работниках и пациентах медицинская организация может получить только от них самих. В случаях когда медицинская организация получает необходимые персональные данные работников и пациентов только у третьего лица, медицинская организация уведомляет об этом работников и пациентов и получает от них письменное согласие.

10.4. Медицинская организация сообщает работникам и пациентам о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работников и пациентов дать письменное согласие на их получение.

10.5. Персональные данные работников и пациентов являются конфиденциальной информацией и не могут быть использованы медицинской организацией или любым иным лицом в личных целях.

10.6. При определении объема и содержания персональных данных работников и пациентов медицинская организация руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

10.7. Медицинская организация разрабатывает меры защиты персональных данных работников и пациентов.

10.8. Работники и пациенты не должны отказываться от своих прав на неприкосновенность частной жизни.

## **XI. Обработка, хранение и передача персональных данных работника и пациента**

11.1. Обработка персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работнику в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работника, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

11.2. Обработка персональных данных пациента осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, установления медицинского диагноза и оказания медицинских услуг.

11.3. Работодатель обрабатывает в информационных системах с использованием средств автоматизации персональные данные работника, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

11.4. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.»:  
- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствует возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;  
- обеспечивает сохранность носителей персональных данных;



- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

11.5. ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» при обработке персональных данных работника или пациента на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;
- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные работников или пациентов.

11.6. В целях обеспечения конфиденциальности документы, содержащие персональные данные работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии медицинской организации, а документы, содержащие персональные данные пациентов, оформляются, ведутся и хранятся только лечащими врачами,

11.7. Работники отдела кадров, бухгалтерии, допущенные к персональным данным работников или пациентов, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных работников или пациентов не допускаются.

11.8. Руководитель отдела кадров вправе передавать персональные данные работника в бухгалтерию организации в случаях, установленных законодательством, необходимых для исполнения обязанностей работников бухгалтерии.

11.9. Руководитель организации может передавать персональные данные работника третьим лицам, только если это необходимо в целях предупреждения угрозы жизни и здоровья работника, а также в случаях, установленных законодательством.

11.10. При передаче персональных данных работника руководитель отдела кадров и руководитель организации предупреждают лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц письменное подтверждение соблюдения этого условия.

11.11. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

11.12. Передача информации, содержащей сведения о персональных данных работников или пациентов, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

11.13. Персональные данные работника хранятся в отделе кадров, в сейфе на бумажных носителях: трудовая книжка, личная карточка и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным работника имеют:

- руководитель организации;
- руководитель отдела кадров организации;
- сотрудники отдела кадров.

11.14. Персональные данные пациента хранятся в картохранилище, на бумажных носителях: медицинская карта и на электронных носителях с ограниченным доступом.

Право доступа к персональным данным пациента имеют: регистратура, лечащие врачи.

11.15. Медицинская организация осуществляет передачу персональных данных работников и пациентов только при наличии согласия указанных лиц на обработку персональных данных, разрешенных ими для распространения.

11.16. Согласие работника или пациента на обработку персональных данных, разрешенных ими для распространения, оформляется отдельно от иных согласий указанного лица на обработку его персональных данных.

11.17. Медицинская организация обеспечивает работникам и пациентам возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных этими лицами для распространения.

11.18. Молчание или бездействие работника или пациента ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных им для распространения.

11.19. В согласии работника или пациента на обработку персональных данных, разрешенных им для распространения, работник или пациент вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных медицинской организацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

Отказ медицинской организации в установлении работником или пациентом запретов и условий, предусмотренных в настоящем пункте, не допускается.

11.20. Медицинская организация в срок не позднее трех рабочих дней с момента получения соответствующего согласия работника или пациента публикует информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных этим работником или пациентом для распространения.

11.21. Установленные работником или пациентом запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных им для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

11.22. Все сведения о передаче персональных данных работников и пациентов учитываются для контроля правомерности использования данной информации лицами, ее получившими.

11.23. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается только в случаях, если работник или пациент дал согласие в письменной форме на обработку своих персональных данных или персональные данные сделаны общедоступными самим субъектом персональных данных.

## **ХII. Требования к помещениям, в которых производится обработка персональных данных**

12.1. Размещение оборудования информационных систем персональных данных, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

12.2. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

## **ХIII. Обязанности медицинской организации по хранению и защите персональных данных работников и пациентов**

13.1. Медицинская организация за свой счет обеспечивает защиту персональных данных работников и пациентов от неправомерного их использования или утраты в порядке, установленном законодательством Российской Федерации.

13.2. Медицинская организация принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами.

Медицинская организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о персональных данных и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам, в частности, относятся:

- 1) назначение ответственного за организацию обработки персональных данных;
- 2) издание документов, определяющих политику медицинской организации в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на медицинскую организацию не предусмотренные законодательством Российской Федерации полномочия и обязанности;
- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Закону о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике медицинской организации в отношении обработки персональных данных, ее локальным актам;
- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Закона о персональных данных, соотношение указанного вреда и принимаемых медицинской организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных названным Федеральным законом;
- 6) ознакомление работников медицинской организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику медицинской организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

13.3. Медицинская организация знакомит работников и их представителей с настоящим положением и их правами в области защиты персональных данных под расписку.

13.4. Медицинская организация осуществляет передачу персональных данных работников и пациентов только в соответствии с настоящим положением и законодательством Российской Федерации.

13.5. Медицинская организация предоставляет персональные данные работников и пациентов только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим положением и законодательством Российской Федерации.

13.6. Медицинская организация не вправе предоставлять персональные данные работников и пациентов в коммерческих целях без их письменного согласия.

13.7. Медицинская организация обеспечивает работникам и пациентам свободный бесплатный доступ к своим персональным данным, включая право на получение копий

любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством.

13.8. Медицинская организация по требованию работника и пациента предоставляет ему полную информацию о его персональных данных и обработке этих данных.

#### **XIV. Права работников и пациентов на защиту их персональных данных**

14.1. Работник или пациент в целях обеспечения защиты своих персональных данных, хранящихся в медицинской организации, имеют право:

- получать полную информацию о своих персональных данных, их обработке, хранении и передаче;
- определять своих представителей для защиты своих персональных данных;
- на доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по их выбору;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями настоящего положения и законодательства Российской Федерации.

При отказе медицинской организации исключить или исправить его персональные данные работник или пациент вправе заявить в письменном виде о своем несогласии с соответствующим обоснованием;

- требовать от медицинской организации извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника или пациента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

14.2. Если работник или пациент считает, что медицинская организация осуществляет обработку его персональных данных с нарушением требований Закона о персональных данных или иным образом нарушает его права и свободы, работник или пациент вправе обжаловать действия или бездействие медицинской организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

14.3. Работник или пациент вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных им для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Закона о персональных данных или обратиться с таким требованием в суд.

#### **XV. Порядок уничтожения, блокирования персональных данных**

15.1. В случае выявления неправомерной обработки персональных данных при обращении работника или пациента медицинская организация осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому работнику или пациенту, с момента такого обращения на период проверки.

15.2. В случае выявления неточных персональных данных при обращении работника или пациента медицинская организация осуществляет блокирование персональных данных, относящихся к этому работнику или пациенту, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы работника или пациента, или третьих лиц.

15.3. В случае подтверждения факта неточности персональных данных медицинская организация на основании сведений, представленных работником или пациентом, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

15.4. В случае поступления требования работника или пациента о прекращении распространения его персональных данных передача (распространение, предоставление, доступ) персональных данных, разрешенных таким работником или пациентом для

- распространения, должна быть прекращена в течение трех рабочих дней с момента получения такого требования.
- Действие согласия работника или пациента на обработку персональных данных, разрешенных им для распространения, прекращается с момента поступления в медицинскую организацию указанного требования.
- 15.5. В случае выявления неправомерной обработки персональных данных, осуществляемой медицинской организацией, медицинская организация в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.
- 15.6. В случае если обеспечить правомерность обработки персональных данных невозможно, медицинская организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.
- 15.7. Об устранении допущенных нарушений или об уничтожении персональных данных медицинская организация уведомляет работника или пациента.
- 15.8. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав работника или пациента, медицинская организация с момента выявления такого инцидента медицинской организацией, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:
- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав работника или пациента, и предполагаемом вреде, нанесенном правам работника или пациента, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном медицинской организацией на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
  - в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).
- 15.9. В случае достижения цели обработки персональных данных медицинская организация прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено трудовым договором или договором на оказание медицинских услуг.
- 15.10. В случае отзыва работником или пациентом согласия на обработку его персональных данных медицинская организация прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено трудовым договором или договором на оказание медицинских услуг.
- 15.11. В случае обращения работника или пациента в медицинскую организацию с требованием о прекращении обработки персональных данных медицинская организация в срок, не превышающий десяти рабочих дней с даты получения ей соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления медицинской организацией в адрес работника или пациента мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.
- 15.12. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.11 настоящего положения, медицинская организация осуществляет блокирование таких персональных данных и обеспечивает уничтожение

персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

15.13. После истечения срока нормативного хранения документов, содержащих персональные данные работника или пациента, или при наступлении иных законных оснований документы подлежат уничтожению.

15.14. Медицинская организация для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

15.15. По результатам экспертизы документы, содержащие персональные данные работника или пациента и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем [указать способ уничтожения: измельчения в шредере/сжигания и т. п.];
- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

#### **XVI. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников и пациентов**

16.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника или пациента, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством Российской Федерации.

16.2. Моральный вред, причиненный работнику или пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Законом о персональных данных, а также требований к защите персональных данных, установленных в соответствии с названным Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником или пациентом убытков.

#### **XVII. Заключительные положения**

17.1. Настоящее положение вступает в силу с момента его утверждения.

17.2. В Положение могут вноситься изменения и дополнения в связи с развитием законодательства Российской Федерации в области персональных данных.

17.3. Положение доводится до работников ГБУЗ ПК «Большесосновская ЦРБ им. Колчановой Г.Ф.» непосредственно осуществляющих обработку персональных данных.