

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ РЕСПУБЛИКИ
ДАГЕСТАН "ХАСАВИЮРТОВСКАЯ ЦЕНТРАЛЬНАЯ ГОРОДСКАЯ БОЛЬНИЦА
ИМ. Р.П. АСКЕРХАНОВА"

УТВЕРЖДАЮ
Главный врач ГБУ РД
«Хасавюртовская ЦГБ им. Р.П.
Аскерханова»



А.Б. Гаджиева

23 декабря 2017 г.

ПОЛОЖЕНИЕ

об обработке и защите персональных данных

Государственное бюджетное учреждение Республики Дагестан
«Хасавюртовская центральная городская больница им. Р.П. Аскерханова»

1. Общие положения

1.1 Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных субъектов, персональных данных учреждения здравоохранения (работников), а также ведения их личных дел.

1.2 Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» и ее работников в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

1.3 Цель настоящего Положения - обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных сотрудников, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.

- Настоящее Положение по **обработке и защите персональных данных** (далее — Положение) в ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» разработано с учётом принципов, правил и требований, установленных основными правовыми нормативными актами:

- Конституция Российской Федерации, принятая 12.12.1993; ст. 23, 24 (неприкосновенность частной жизни, личная и семейная тайна), ст. 41, 42 (недопустимость сокрытия информации, связанной с угрозой жизни и здоровью);

- Гражданским кодексом Российской Федерации;

- Федеральным законом от 21.11.2011 № 323-ФЗ (ред. от 29.07.2017)

"Об основах охраны здоровья граждан в Российской Федерации" (Статья 13. Соблюдение врачебной тайны)

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации», в котором даны определения понятий: информация, документирование информации, защита информации, обладатель информации, конфиденциальность информации, предоставление и распространение информации, электронное сообщение;

- Федеральный закон "О персональных данных" № 152-ФЗ от 27.07.2006;

- Указ Президента РФ от 06 марта 1997 г. № 188 Об утверждении перечня сведений конфиденциального характера (с изменениями на 13 июля 2015 года);

- Постановление Правительства РФ от 17.11.07 № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", в котором определены основные требования к указанным информационным системам (ИС).

- Указ Президента РФ № 351 от 17.03.2008 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";

- Постановление Правительства РФ от 03.02.2012 N 79 (ред. от 15.06.2016) "О лицензировании деятельности по технической защите конфиденциальной информации" (вместе с "Положением о лицензировании деятельности по технической защите конфиденциальной информации")

- Постановление Правительства РФ от 16.04.2012 № 313 (ред. от 18.05.2017) "Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)";

- Постановление Правительства РФ от 06.07.2008 № 512 (ред. от 27.12.2012) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне

информационных систем персональных данных”;

- Постановление Правительства РФ № 687 от 15.09.2008 “Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации”;

- Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 23.03.2017) “Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных” (Зарегистрировано в Минюсте России 14.05.2013 № 28375);

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 14 февраля 2008 г.);

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15 февраля 2008 г.);

- “Методический документ. Меры защиты информации в государственных информационных системах”(утв. ФСТЭК России 11.02.2014)

- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

- ГОСТ Р ИСО/МЭК 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

- ГОСТ 34.603-92 Виды испытаний автоматизированных систем.

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных” (Выписка)(утв. ФСТЭК РФ 15.02.2008)

- Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В.Симаковым, согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В.Куц).

- Трудовой кодекс Российской Федерации” от 30.12.2001 № 197-ФЗ (ред. от 29.07.2017 (Глава 14. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА).

- Федеральный закон от 29 июля 2004 года № 98-ФЗ “О коммерческой тайне”

1.4 Упорядочение обращения с персональными данными имеет целью обеспечения в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных работников лечебно-профилактического учреждения (ЛПУ); защиты интересов третьих лиц, с

которыми заключены договора, содержащие конфиденциальную информацию, доступ к которым ограничен, а также в обращениях граждан и иных субъектов персональных данных от несанкционированного доступа и разглашения.

1.5 Настоящее положение обязательно для всех работников ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова», получающих доступ к сведениям, составляющим персональные данные, медицинскую и коммерческую тайну.

1.6 Режим конфиденциальности в отношении персональных данных снимается:

- в случае их обезличивания;
- по истечении срока их хранения;
- в других случаях, предусмотренных федеральными законами.

1.7 Целью настоящего Положения является определение порядка обработки персональных данных работников ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» согласно перечню персональных данных, утвержденного приказом главного врача (Приложение № 6 к настоящему Положению); обеспечение защиты их прав и свобод при обработке персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

1.8 Персональные данные относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере негосударственной (служебной, профессиональной) тайны.

1.9 Настоящее Положение и изменения к нему вступают в силу с момента его принятия и применяется к отношениям, возникшим после введения его в действие.

2. Основные понятия и состав персональных данных

2.1 Для целей настоящего Положения используются следующие основные понятия и определения:

- **«персональные данные»**- любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

- **«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;

- **«субъект»** - субъект персональных данных;

- **«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;

- **«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;

- **«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;

- **«обезличивание персональных данных»**- действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

- **«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;

- **«конфиденциальность персональных данных»**- обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

- **«конфиденциальная информация»**- это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.

- **«трансграничная передача персональных данных»** - передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

- **«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;

- **«информация»** - сведения (сообщения, данные) независимо от формы их представления.

- **«доступ к информации»**- возможность получения информации и ее использования;

- **«документированная информация»** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

- **«медицинская тайна»** - это информация о состоянии здоровья

пациента, полученная при его обращении за медицинской помощью, в процессе обследования и лечения, в отношении которой введен режим конфиденциальности.

- **«персональные данные пациента»** - это любая информация о пациенте и членах его семьи, полученная при обращении за медицинской помощью, обследовании и лечении.

- **«неуполномоченное лицо»** - лицо, не имеющее допуска к информации.

- **«блокирование персональных данных»** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

- **«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.

3. Состав персональных данных, обрабатываемых с использованием

3.1 К персональным данным ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» относятся:

3.1.1 Персональные данные работника - любая информация, относящаяся к данному работнику (субъекту персональных данных) и необходимая ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» в связи с трудовыми отношениями, в том числе:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- анкета;
- автобиография;
- сведения и копии документов об образовании;
- сведения о трудовом и общем стаже;
- сведения о предыдущем месте работы;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- реквизиты полиса медицинского страхования;
- сведения о наличии льгот;
- данные о состоянии здоровья;
- сведения о случаях обращения за медицинской помощью;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний (мобильный) телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;

- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей (для ряда должностей);
- фотографии;
- другая информация, определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений.

3.2 Перечень персональных данных автоматизированной информационной системы ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» зависит от категории субъекта персональных данных и утверждается руководителем Организации

4. Общие принципы обработки персональных данных

4.1 Обработка персональных данных осуществляется на основе принципов:

- Обработка персональных данных должна осуществляться на законной и справедливой основе.
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- Обработке подлежат только персональные данные, которые отвечают целям их обработки.
- Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
- При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные

подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством.

5. **Общедоступные источники персональных данных**

5.1 В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъектов могут включаться:

его фамилия, имя, отчество, число, месяц и год рождения, адрес, телефон, сведения о профессии и иные персональные данные, представленные субъектом.

5.2 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.

6. **Субъекты персональных данных**

6.1 Субъектам персональных данных являются следующие категории физических лиц:

- пациенты и их представители;
- работники ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова»;
- кандидаты для приема на работу.

7. **Обязанности работников**

7.1 Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных представлена в приложении № 1 настоящего положения.

7.2 Обеспечивая конфиденциальность, работник обязуется:

- знать и соблюдать требования по получению, обработке, передаче, хранению, получению сведений, составляющих профессиональную тайну и персональные данные пациентов, предусмотренные нормативными правовыми актами, коллективным договором, соглашениями, должностной инструкцией, локальными нормативными актами ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» и трудовым договором;

- принимать меры по установлению и сохранению режима конфиденциальности, предусмотренные нормативными правовыми актами, коллективным договором, соглашениями, должностной инструкцией, локальными нормативными актами ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» и трудовым договором;

- не использовать без разрешения обладателя или субъекта персональных данных **информацию ограниченного доступа** в целях, не связанных с осуществлением трудовой функции;

- не разглашать сведения, составляющие медицинскую тайну и персональные данные пациентов, а также не совершать иных деяний, влекущих уничтожение или утрату таких сведений (их материальных носителей) или

потерю ее коммерческой или иной ценности для ее обладателя;

- незамедлительно сообщать об утрате или несанкционированном уничтожении сведений, составляющих медицинскую тайну и персональные данные, своему непосредственному руководителю, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности таких сведений (в том числе о попытках неправомерного доступа к информации со стороны неуполномоченных лиц);

- обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с работниками по оплате труда, медицинская документация и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные;

- заполнение документации, содержащей персональные данные работника, осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.04 №1 или в соответствии с разработанными формами документов по учетной политике в учреждении

7.3 Работники **обязаны проходить обучение и проверку знаний** требований по обеспечению конфиденциальности информации не реже, чем один раз в 12 месяцев.

7.4 При прекращении трудовых отношений с ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» работник обязан сдать все материальные носители сведений, содержащие медицинскую тайну и персональные данные, а также ключи от помещений и шкафов, в которых они хранятся.

7.5 Сотрудники **отдела информационного обеспечения и автоматизации** обеспечивают следующие меры по защите хранящейся на сервере информации:

- ограничение сетевого доступа на сервер для определенных пользователей;

- организацию в отдельном сегменте сети всех компьютеров пользователей и серверов с ограниченным доступом;

- организацию контроля технического состояния серверов и уровней защиты и восстановления информации;

- проведение регулярного резервного копирования информации;

7.6 ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации; Защита персональных данных работников и пациентов в ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» возлагается на:

➤ главного врача;

➤ заместителей главного врача ;

➤ на всех работников отделов, служб, управлений;

➤ главного бухгалтера;

➤ работников отдела кадров (ведение трудовых книжек, личных карточек формы Т- 2, личных дел);

- работников бухгалтерии (ведение документации по учету труда и его оплате);
- работников планово-экономического отдела;
- инженера по охране труда;
- программистов;
- операторов электронно-вычислительных машин;
- главного специалиста по защите информации;
- председателя профсоюзного комитета;
- руководителей структурных подразделений;
- старших медицинских сестер отделений;
- врачей и средний медицинский персонал.

7.7 Защита персональных данных представляет собой жестко регламентированный и динамически-технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

7.8 Защита персональных данных работников и пациентов от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами.

8. Требования по получению, обработке, хранению и использованию информации ограниченного доступа

8.1 Персональные данные субъектов персональных данных могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде. Порядок хранения анкет и иных документов, содержащих информацию персонального характера, а также согласий на обработку персональных данных определяются «Положением о порядке хранения информации персонального характера на бумажных носителях»

8.2 Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства. Сбор и обработка персональных данных осуществляется исключительно с письменного согласия субъекта. Образцы форм заявления о согласии на обработку персональных данных и отказа от нее, размещены в Приложении №3, Приложении № 4 и Приложении № 5. Персональные данные субъекта ПД относятся к конфиденциальной информации. Требования при обработке персональных данных работника установлены ст. 86 Трудового кодекса РФ и не подлежат изменению и исключению.

8.3 Обработка персональных данных субъекта может осуществляться

исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, наблюдения и лечения пациентов и обеспечения сохранности имущества оператора, работника (пациента) и третьих лиц.

8.4 Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

8.5 В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, **не превышающий трех рабочих дней** с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. **В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные** или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта обработки персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

8.6 В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8.7 Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников (медицинских карт для пациентов), которые хранятся в личном деле в отделе кадров (регистратуре, архиве). Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах

получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

8.8 Письменное согласие не требуется, если обработка персональных

данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

8.9 Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом №152-ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона №152-ФЗ «О персональных данных».

8.10 Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

8.11 В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

8.12 Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

8.13 Оператор обязан рассмотреть возражение в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

8.14 Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

8.15 Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных

федеральными законами.

8.16 При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами.

8.17 При поступлении на работу работник представляет сотрудникам отдела кадров следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о регистрации индивидуального налогового номера (ИНН);
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

8.18 При оформлении работника отделом кадров заполняется унифицированная форма Т-2 "Личная карточка работника", в которой отражаются следующие анкетные и биографические данные работника:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;
- сведения об аттестации;
- сведения о повышенной квалификации;
- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и о контактных телефонах.

8.19 Запрещается требовать от лица, поступающего на работу (или прием), документы помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

8.20 При заключении трудового договора и в ходе трудовой деятельности может возникнуть необходимость в предоставлении служащим документов:

- о возрасте детей;
- об инвалидности;
- о донорстве;
- о составе семьи;
- о необходимости ухода за больным членом семьи;
- прочие.

8.21 После того, как будет принято решение о приеме работника на работу,

а также впоследствии в процессе трудовой деятельности, к документам, содержащим персональные данные субъекта, также будут относиться:

- трудовой договор;
- приказ о приеме на работу;
- приказы о поощрениях и взысканиях;
- медицинский осмотр сотрудника при приеме на работу (флюорограмма грудной клетки, анализ крови на RW, ВИЧ, гепатиты);
- приказы, связанные с прохождением учебы сотрудников;
- карточка унифицированной формы Т-2, утвержденная постановлением Госкомстата России от 05.01.04 №1;
- другие документы согласно законодательству Российской Федерации

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

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

8.24 Во время приема пациента не допускается нахождение на рабочем столе медицинских документов (амбулаторных карт, результатов анализов и т.п.), не относящихся к принимаемому в данный момент пациенту.

8.25 Субъекты или их законные представители должны быть ознакомлены под расписку с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

8.26 В целях обеспечения достоверности персональных данных субъект обязан:

8.26.1. При приеме на работу (к врачу) предоставить оператору полные достоверные данные о себе.

8.26.2. В случае изменения сведений, составляющих персональные данные, работник незамедлительно должен предоставить данную информацию в отдел кадров учреждения здравоохранения.

8.27 Не допускается сообщение сведений о состоянии здоровья пациента, диагнозе его заболевания и др. сведений о пациенте с использованием средств связи (телефон, факс, Интернет и т.п.).

8.28 При отсутствии согласия субъекта обработка общих категорий персональных данных допускается в случае, если:

- осуществляется на основании и во исполнение федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется в статистических или иных научных целях при условии обязательного обезличивания персональных

данных;

8.29 Обработка персональных данных осуществляется:

- без использования средств автоматизации;
- с использованием автоматизированной информационной системы;

8.30 Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно; При отсутствии согласия субъекта обработка специальных категорий персональных данных в соответствии с Законом № 152-ФЗ обработка специальных категорий допускается в случае, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья субъекта персональных данных, и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка данных производится лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну;

- обработка персональных данных необходима в связи с осуществлением правосудия (запрос из суда, прокуратуры);

- обработка персональных данных осуществляется в соответствии с законодательством РФ 6. о безопасности, оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством РФ.

8.31 При передаче персональных данных пациентов третьим лицам должны быть соблюдены следующие требования:

- персональные данные предоставляются только с письменного согласия пациента, за исключением случаев, предусмотренных федеральным законом;

- предупреждение лиц, получивших доступ к персональным данным пациента о возможности использования сведений только в установленных целях и об ответственности за нарушение законодательства в этой сфере;

- соблюдение режима конфиденциальности получателями.

8.32 Не допускается передача и выдача документов, содержащих медицинскую тайну и персональные данные пациента, **неуполномоченным лицам.**

Передача соответствующих документов в регистратуру возможна только самим лечащим врачом или медицинским персоналом, имеющим допуск к такой информации.

8.33 При регистрации пациента и выдачи ему амбулаторной карты, стационарной карты и иных документов, касающихся состояния его здоровья,

также должна обеспечиваться конфиденциальность.

8.34 Хранение сведений, составляющих медицинскую тайну и персональные данные пациентов, осуществляется в порядке, исключающем их утрату, неправомерное использование или получение доступа неуполномоченными лицами, только в соответствии с целями, определившими их получение.

8.35 Стационарные карты, амбулаторные карты подлежат сдаче в архив, регистратуру для их последующего хранения. *Не допускается доступ в помещение для хранения неуполномоченных лиц.* Двери помещения для хранения после окончания рабочего дня закрываются и опечатываются. В течение рабочего дня не допускается оставлять данное помещение открытым.

8.36 Персональные данные субъектов хранятся на бумажных носителях в помещении отдела кадров (регистратуре). Для этого используются специально оборудованные шкафы и сейфы.

8.37 Личные дела уволенных (прошедших обследование, лечение) субъектов хранятся в архиве учреждения здравоохранения (Срок хранения определяется действующим нормативным документом).

8.38 Сведения о начислении и выплате заработной платы работникам учреждения здравоохранения хранятся на бумажных носителях в помещении расчетного отдела бухгалтерии. По истечении сроков хранения, установленных законодательством РФ, данные сведения передаются в архив учреждения здравоохранения.

8.39 Конкретные обязанности по ведению, хранению личных дел субъектов, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные субъектов, возлагается *на работников отдела кадров, а по хранению личных дел уволенных (обследованных, пролеченных) субъектов* - на работников архива и закрепляются в должностных инструкциях.

8.40 Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, *предусмотренном архивным законодательством Российской Федерации.*

8.41 Сведения о субъектах ПД учреждения здравоохранения хранятся также на электронных носителях - в базах данных РМИАС Промед, АИС 1С: Зарплата + Кадры; передача информации по внутренней сети и сети Интернет; операции с персональными данными: сбор, хранение, накопление, уточнение, передача, уничтожение данных.

8.42 При получении сведений, составляющих персональные данные субъектов заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

8.43 Все медицинские документы, результаты анализов должны

храниться в шкафах, оборудованных замками и закрытых помещениях. Все помещения, в которых хранятся материальные носители информации ограниченного доступа, после окончания рабочего дня опечатываются.

8.44 Использование сведений, составляющих медицинскую тайну или персональные данные пациентов, допускается только в целях обследования и лечения пациентов в ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова».

8.45 Не допускается использовать информацию о пациентах за пределами рабочего времени и (или) в целях, не связанных с осуществлением своих трудовых обязанностей в ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова», а также после прекращения трудовых отношений с ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова».

8.46 Вынос резервных и технологических копий баз данных автоматизированной информационной системы, содержащих информацию персонального характера, из организации запрещен. Передача и копирование резервных и технологических копий баз данных допустима только для прямого использования с целью технологической поддержки автоматизированной информационной системы.

8.47 Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения руководителя или уполномоченного им лица.

8.48 Хранение резервных и технологических копий баз данных автоматизированной информационной системы, содержащих информацию персонального характера, осуществляется на серверах организации и сменных носителях, доступ к которым ограничен.

8.49 При принятии решений, затрагивающего интересы субъекта персональных данных, нельзя основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

9. Права и обязанности субъектов в целях защиты персональных данных

9.1 Для своевременной и полной реализации своих прав, субъект обязан предоставить организации-оператору достоверные персональные данные.

9.2 Субъекты персональных данных не должны отказываться от своих прав на сохранение и защиту тайны.

9.3 В целях обеспечения защиты персональных данных, хранящихся у оператора, субъекты имеют право на:

9.3.1 Полную и безвозмездную информацию об их персональных данных и обработке этих данных.

9.3.2 Субъект имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

9.3.2.1 подтверждение факта обработки персональных данных оператором;

9.3.2.2 правовые основания и цели обработки персональных данных;

9.3.2.3 цели и применяемые оператором способы обработки персональных данных;

9.3.2.4 наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

9.3.2.5 обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

9.3.2.6 сроки обработки персональных данных, в том числе сроки их хранения;

9.3.2.7 порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

9.3.2.8 информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9.3.2.9 наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

9.3.2.10 иные сведения, предусмотренные Федеральным законом №152-ФЗ «О персональных данных» или другими федеральными законами.

9.3.3 Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом.

9.3.4 В случае, если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления субъект по его запросу, субъект вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

9.3.5 Определение своих представителей для защиты своих персональных данных.

9.3.6 Сведения предоставляются субъект или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись пациента или его представителя. **Запрос может быть направлен в форме электронного документа и подписан электронной подписью** в соответствии с

законодательством Российской Федерации.

9.3.7 Субъект вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

9.3.8 Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе оператора исключить или исправить персональные данные субъекта он имеет право заявить в письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.

9.3.9 Требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.

9.3.10 Если субъект считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального Закона № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие организации-оператора в уполномоченный орган по защите прав субъектов персональных данных (Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи) или в судебном порядке.

9.3.11 Субъект имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

9.3.12 Обжалование в суд любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

10. Передача персональных данных пациентов третьим лицам

10.1 Передача персональных данных пациентов третьим лицам осуществляется организацией-оператором только с их письменного согласия, за исключением случаев, если:

10.1.1 передача необходима для защиты жизни и здоровья пациента либо других лиц, и получение его согласия невозможно;

10.1.2 по запросу органов дознания, следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством, в соответствии с Законом об оперативно-розыскной деятельности, после официальной визы руководителя учреждения о передаче персональных данных на запросе;

10.1.3 при наличии оснований, позволяющих полагать, что права и интересы пациента могут быть нарушены противоправными действиями других лиц;

10.1.4 в иных случаях, прямо предусмотренных федеральными законами.

10.2 Сбор и передача персональных данных, копий документов у работников, по запросу третьих лиц, не предусмотренных для обработки и хранения не допускается.

10.3 Передача персональных данных **пациента третьим лицам** осуществляется на основании запроса третьего лица с **разрешающей визой главного врача** или **лица, осуществляющего** его обязанности на основании **Приказа главного врача**. Организация-оператор обеспечивает ведение Журнала учета выданных персональных данных пациента, в котором регистрируются поступившие запросы, **фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана**. Факт поступления запроса/заявления, содержание запрашиваемых персональных данных, а также **согласие пациента на их передачу фиксируется** уполномоченным лицом работодателя, назначенного Приказом «О назначении ответственных лиц», в Журнал учета выданных персональных данных пациентов **по запросам третьих лиц (органов прокуратуры, внутренних дел, службы судебных приставов, организаций и т.п.)**.

10.4 В случае если лицо, **обратившееся с запросом, не уполномочено федеральными законами на получение персональных данных** пациента, либо отсутствует **письменное согласие пациента на передачу** его персональных данных, организация-оператор обязана отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, **выдается мотивированный отказ** в предоставлении персональных данных в письменной форме, копия отказа хранится у организации-оператора.

11. Порядок передачи персональных данных субъектов ПД

11.1 Доступ сотрудников к конфиденциальной информации, содержащейся как в автоматизированной информационной системе организации, так и на бумажных носителях осуществляется с **письменного согласия руководителя учреждения или уполномоченного им лица (допуск)**.

11.2 Сотрудник, получивший допуск к конфиденциальной информации, должен **быть ознакомлен с настоящим Положением**.

11.3 При получении доступа к конфиденциальной информации сотрудники **подписывают соответствующие соглашения** о неразглашении данной информации.

11.4 Доступ к автоматизированной информационной системе учреждения разграничен политикой безопасности системы, реализуемой с использованием технических и организационных мероприятий.

11.5 Каждый пользователь имеет **индивидуальную учетную запись**, которая определяет его права и полномочия в автоматизированной информационной системе. **Информация об учетной записи не может быть передана другим лицам**. Пользователь несет персональную ответственность за **конфиденциальность сведений собственной учетной записи**.

11.6 Запрещается использование для доступа к автоматизированной информационной системе Организации учетных записей других пользователей.

11.7 Созданием, удалением и изменением учетных записей пользователей автоматизированной информационной системы занимаются **уполномоченные администраторы** в соответствии с должностными обязанностями.

11.8 Право доступа к персональным данным субъектов персональных данных в части их касающейся имеют:

- главный врач;
- заместители главного врача;
- главный бухгалтер;
- сотрудники бухгалтерии (ведение документации по учету труда и его оплате);
- сотрудники отдела кадров (ведение трудовых книжек, личных карточек формы Т- 2, личных дел);
- сотрудники экономической службы;
- инженер по охране труда;
- главный специалист по защите информации;
- председатель профсоюзного комитета;
- сотрудники канцелярии (информация о фактическом месте проживания и контактные телефоны работников);
- руководители структурных подразделений по направлению деятельности
- медицинский персонал, включая врачей, средний и младший медицинский персонал, а также лиц, проходящих стажировку и обучение в объеме необходимом и достаточном для успешного выполнения профессиональной деятельности;

11.9 Управление по организации и контролю за медицинской деятельностью

11.10 Отдел информационного обеспечения и автоматизации;

11.11 Управление кадровой службы и правового обеспечения ЦГБ;

11.12 Работники отдела кадров;

11.13 Юрисконсульт;

11.14 Работники планово-экономического отдела;

11.15 Работники бухгалтерии.

11.16 При передаче персональных данных субъектов сотрудники ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова», имеющие доступ к персональным данным, должны соблюдать следующие требования:

11.9.1 Не сообщать персональные данные субъекта третьей стороне без письменного согласия работника субъекта, 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. Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта, оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора,

отсутствует угроза жизни или здоровью субъекта, оператор обязан отказать в предоставлении персональных данных лицу.

11.9.2 Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

11.9.3 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.

11.9.4 Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

11.9.5 Все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается какая именно информация была передана. Форма журнала учета передачи персональных данных представлена в приложении № 2 к настоящему Положению.

11.9.6 Передавать персональные данные работника представителю работника в порядке, установленном Трудовым кодексом РФ и настоящим Положением, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанным представителем его функций.

11.17 При получении доступа к персональным данным субъектов сотрудники подписывают Обязательство о неразглашении персональных данных.

11.18 К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, областных и муниципальных органов управления. Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции.

12. Организация конфиденциального делопроизводства

12.1 Все документы, содержащие информацию ограниченного доступа, должны сохраняться в режиме конфиденциальности и быть доступными только тем лицам, которые имеют допуск к таким сведениям в силу исполнения ими своих должностных обязанностей.

Организация конфиденциального делопроизводства должна исключать ознакомление с информацией иных лиц, не имеющих такого доступа.

12.2 На документах конфиденциального характера в правом верхнем углу первого листа ставится гриф «**Конфиденциально**» с указанием номера

экземпляра. На обороте листа (обложки) документа с грифом «Конфиденциально» указываются **Список лиц, которые вправе использовать документ при осуществлении своей трудовой функции**

12.3 Приказом по ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» назначается **группа лиц, ответственных за учет, хранение и использование информации, ограниченного доступа.**

12.4 Документы и иные материальные носители, содержащие конфиденциальную **информацию, хранятся в сейфе** или ином закрытом помещении, приспособлении, к которому отсутствует свободный доступ других лиц.

12.5 Движение документов с грифом «Конфиденциально» должно своевременно отражаться в **«Журнале учета движения конфиденциальных документов ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова».**

12.6 При работе с документами, имеющими гриф «Конфиденциально» **запрещено:**

- **делать выписки в целях, не связанных с оказанием** медицинской помощи пациенту или не связанных с осуществлением трудовой функции;
- **знакомить с такими документами, в том числе в электронном** виде других лиц, не имеющих соответствующего доступа;
- **использовать информацию из таких документов в открытых** сообщениях, докладах, переписке, рекламных изданиях (такое использование допускается только **при условии обезличивания информации;**
- **оставлять на рабочем месте документы и иные носители** информации с грифом «Конфиденциально»;
- **не допускать к компьютерам, содержащим персональные данные** пациентов и медицинскую тайну, **посторонних лиц;**
- **не оставлять включенными компьютеры,** содержащие персональные данные пациентов и медицинскую тайну.

13. Особенности предоставления доступа к персональным данным

13.1 При передаче конфиденциальных данных учреждение должно соблюдать следующие **требования:**

13.2 Не сообщать данные третьей стороне **без письменного согласия соответствующего лица,** за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом.

13.3 Не сообщать данные в коммерческих целях без его письменного согласия другой стороны.

13.4 **Предупредить лиц, получивших конфиденциальную информацию,** о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие данные, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными пациентов в порядке, установленном федеральными законами.

13.5 Осуществлять передачу конфиденциальных данных в пределах ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» в соответствии с настоящим Положением и Положениями о защите персональных данных работников и пациентов.

13.6 Разрешать доступ к конфиденциальной информации только специально уполномоченным лицам, при этом **указанные лица должны иметь право получать только те данные, которые необходимы для выполнения конкретной функции.**

13.7 Передавать персональные данные работников и пациентов его законным, полномочным представителям в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции. **Конфиденциальную информацию по Договорам передавать третьим лицам согласно условиям Договора.**

13.8 Внешний доступ

13.8.1 К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции; правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- ТФОМС, СМО
- пенсионные фонды;
- подразделения муниципальных органов управления;
- органы исполнительной власти.

13.8.2 Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

13.8.3 Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

13.8.4 Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

13.9 Персональные данные работников и пациентов обрабатываются и хранятся в АСУ, отделе кадров, архиве учреждения. Конфиденциальная информация по Договорам хранятся в юридическом отделе учреждения.

13.10 Персональные данные работников и пациентов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной

компьютерной сети).

13.11 При получении персональных данных не от работника или пациента (за исключением случаев, если персональные данные являются общедоступными) учреждение до начала обработки таких персональных данных обязан предоставить этому лицу следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

- цель обработки персональных данных и ее правовое основание;

- предполагаемые пользователи персональных данных;

- установленные федеральными законами права субъекта персональных данных.

14. Ответственность за нарушение норм, регулирующих обработку и защиту конфиденциальной информации

14.1 К видам нарушения режима конфиденциальности относятся:

- разглашение информации, составляющей медицинскую тайну, персональные данные работников и пациентов; разглашение условий и содержания Договора, предусматривающего режим конфиденциальности.

- неправомерное использование информации, составляющей конфиденциальную информацию (использование без согласия субъекта и (или) в целях, не связанных с оказанием медицинской помощи пациенту в ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова».

- утрата документов и иных материальных носителей сведений, составляющих конфиденциальную информацию в соответствии с разделом настоящего положения;

- неправомерное уничтожение документов, содержащих конфиденциальную информацию;

- нарушение требования хранения документов, содержащих конфиденциальную информацию (хранение в открытом доступе, оставление на рабочем столе и т.д.);

- передача документов и сведений, составляющих конфиденциальную информацию неуполномоченным лицам;

- другие нарушения требований законодательства и настоящего Положения.

14.2 Нарушение требований законодательства об обеспечении конфиденциальности влечет наступление уголовной, административной, дисциплинарной, материальной и гражданско-правовой ответственности. Уголовная, административная и гражданско-правовая ответственность наступает в установленных законом случаях.

14.3 Разглашение конфиденциальную информацию может являться основанием для расторжения трудового договора с работниками ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» по подпункту «в» пункта 6 части первой статьи 81 Трудового кодекса Российской Федерации. Работники ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова», виновные в нарушении порядка обращения с конфиденциальной информацией, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в

соответствии с федеральными законами. Неоднократное нарушение требований режима конфиденциальности может послужить основанием для прекращения трудового договора по пункту 5 части первой статьи 81 Трудового кодекса Российской Федерации.

14.4 ГБУ РД «Хасавюртовская ЦГБ им. Р.П. Аскерханова» за нарушение порядка обращения с конфиденциальной информацией несет ответственность согласно действующему законодательству РФ.

14.5 Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

15. Заключительные положения

15.1 Настоящее Положение вступает в силу с момента его утверждения главным врачом медицинского учреждения.

15.2 Настоящее Положение доводится до сведения всех субъектов ПД медицинского учреждения

Начальник управления кадровой
службы и правового обеспечения



Н.М. Магомедов

Юрисконсульт



А.И. Аджиев