УТВЕРЖДАЮ
И.о. главного врача
ГБУЗ РБ ГКБ №13 г. Уфа
_____И.В. Борисов
_____2017 г.

Приложение №3
к приказу по ГБУЗ РБ ГКБ № 13
г. Уфа
от 07.12.2017 г. № 574 – ОД

Положение о защите персональных данных пациентов и работников ГБУЗ РБ ГКБ № 13 г. Уфа

Уфа 2017

СОДЕРЖАНИЕ

Содержание 2
Определения 3
Обозначения и сокращения 5
Общие положения 6
Принципы организации работ по защите персональных данных 8
Доступ к персональным данным 8
Требования к помещениям 10
Общие требования по обработке персональных данных 11
Общие требования по организации безопасной работы в информационных системах персональных данных 14
Учет 16
Хранение 17
Уничтожение 19
Передача 20
Ответственность за разглашение конфиденциальной информации, связанной с персональными данными 24
Приложение 1 27
Приложение 2 28
Приложение 3 30
Приложение 4 31

ОПРЕДЕЛЕНИЯ

Для целей Положения по организации и проведению работ по обеспечению безопасности персональных данных (далее – Положение) используются следующие термины и определения:

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

Допуск к информации – официальное разрешение субъекту обращаться к информации определенного уровня конфиденциальности.

Информация – сведения (сообщения, данные) независимо от формы их представления;

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;

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;

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

Несанкционированный доступ к информации – неправомерное получение, использование, утрата, уничтожение, искажение, блокирование информации.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации лицу, в том числе его

фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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

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;

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;

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;

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;

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУИ – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

Общие положения

1.1. Целью данного Положения является обеспечение прав и свобод человека и гражданина в отношении их персональных данных путем определения принципов, правил и методов защиты персональных данных от несанкционированного доступа при их обработке в ГБУЗ РБ ГКБ № 13 г. Уфа (далее – Учреждении), в том числе при передаче персональных данных третьим лицам.

1.2. Настоящее Положение разработано в соответствии с:

1.2.1. Конституцией Российской Федерации;

1.2.2. Гражданским кодексом Российской Федерации;

1.2.3. Трудовым кодексом Российской Федерации;

1.2.4. Кодексом об административных правонарушениях;

1.2.5. Уголовным кодексом РФ;

1.2.6. Федеральным законом от 27 июля 2006 года N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

1.2.7. Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

1.2.8. Постановление Правительства РФ от 1.10.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

1.2.9. Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15 сентября 2008 г. № 687;

1.2.10. Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2.141.2.11 Приказ 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".

1.2.151.2.12 Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

1.2.161.2.13 Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

1.2.17 Уставом Учреждения;

1.2.15 Правилами внутреннего распорядка Учреждения;

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным сотрудников и пациентов (далее – субъекты персональных данных).

1.5. Настоящее Положение вступает в силу с момента его утверждения главным врачом Учреждения и действует бессрочно, до замены его новым Положением.

1.6. Все изменения в Положение вносятся приказом главного врача.

1.7. Контроль исполнения данного Положения осуществляет сотрудник, ответственный за обеспечение информационной безопасности.

Принципы организации работ по защите персональных данных

Для обеспечения защиты персональных данных следует руководствоваться следующими принципами:

2.1. Ограничение и регламентация состава работников, функциональные обязанности которых требуют работы с конфиденциальными сведениями;

2.2. Строгое избирательное и обоснованное распределение документов и информации между работниками;

2.3. Рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

2.4. Знание и выполнение работником требований нормативно-методических документов по защите информации и сохранению тайны;

2.5. Наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

2.6. Определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

2.7. Организация порядка уничтожения информации;

2.8. Своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

2.9. Воспитательная и разъяснительная работа с сотрудниками подразделений по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

2.10. Система защиты информации не должна значительно затруднять технологический процесс.

Доступ к персональным данным

3.1. К работе с персональными данными, обрабатываемыми в Учреждении, должны допускаться только сотрудники, имеющие документально оформленный допуск.

3.2. Допуск сотрудников Учреждения осуществляется в соответствии с перечнями допущенных по подразделениям, составляемых руководителями структурных подразделений и утверждаемых главным врачом.

3.3. Для получения допуска руководители структурных подразделений готовят на имя главного врача раппорт на допуск сотрудников своих подразделений к персональным данным (Приложение 1).

3.4. В раппорте должны быть указаны фамилия, имя, отчество сотрудника, его должность, перечень сведений, содержащих персональные данные, и информационных систем персональных данных к которым работнику необходим доступ для выполнения своих должностных обязанностей.

3.5. На основании раппорта готовится перечень сотрудников подразделения, допущенных к обработке персональных данных, который утверждается главным врачом Учреждения.

3.6. Перечень сотрудников подразделения, допущенных к обработке персональных данных, должен храниться в Канцелярии.

3.7. Сотрудники подразделения должны быть ознакомлены с данным перечнем под роспись.

3.8. Копия либо выписка из перечня заверяется сотрудником Канцелярии и передается в соответствующее структурное подразделение, где хранится у руководителя.

3.9. Доступ к автоматизированным рабочим местам, входящим в состав ИСПДн, осуществляется в соответствии с матрицей доступа, зафиксированной в Положении о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн ГБУЗ РБ ГКБ № 13 г. Уфа. Матрица доступа составляется на основании Отчета о результатах проведения внутренней проверки и утвержденного перечня допущенных лиц.

3.10. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных. (Приложение 2).

Требования к помещениям

4.1. В помещениях, в которых в рабочее время осуществляется прием посетителей и одновременно ведется обработка персональных данных, должно быть установлено разграничение на 2 зоны: зона А, в которой предусматривается нахождение посетителей и зона Б, в которой предполагается обрабатывать персональные данные.

4.2. Разграничение на зоны должно производиться путем установки физического препятствия, которое затрудняет проникновение к рабочим местам сотрудников в зоне Б (например, мебельные стойки, двери, окна касс).

4.3. В исключительных случаях, когда в силу специфики работы установка подобных барьеров невозможна, посетители могут находиться в помещении в специально выделенное для приема посетителей время при обязательном присутствии сотрудника подразделения. Сотрудники на время приема посетителей не осуществляют работу с персональными данными. Все документы, содержащие персональные данные, кроме тех, которые не относятся к конкретному посетителю, должны быть убраны в папки или шкафы (сейфы).

4.4. В зоне Б разрешается находиться только сотрудникам, которым в установленном порядке оформлен допуск к соответствующей конфиденциальной информации (персональным данным).

4.5. В нерабочее время помещения, в которых ведется обработка персональных данных, должны запираться на ключ.

4.6. Контроль доступа лиц в помещение зоны Б обеспечивается сотрудниками подразделения.

4.7. Не допускается бесконтрольное нахождение посторонних лиц в помещениях, в которых ведется обработка персональных данных.

4.8. Оргтехника должна располагаться таким образом, чтобы обеспечивать невозможность просмотра из зоны А информации выводимой на экраны мониторов и на печать.

4.9. Помещение, где в нерабочее время происходит хранение носителей конфиденциальной информации, должно быть оборудовано охранной и пожарной сигнализацией.

4.10. Окна в помещении оборудуются жалюзи или шторами, которые при работе с персональными данными должны быть закрыты.

4.11. Сдачу под охрану и снятие с охраны помещений подразделения Учреждения осуществляют сотрудники данного подразделения, назначенные заведующим подразделением. Помещение сдается под охрану с записью в соответствующем журнале у вахтера на входе в здание Учреждения.

4.12. Присутствие обслуживающего персонала Учреждения, в том числе уборка помещений, допускается строго в присутствии хотя бы одного из сотрудников подразделения.

Общие требования по обработке персональных данных

5.1. Обработка персональных данных в ГБУЗ РБ ГКБ № 13 г. Уфа должна осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъектам персональных данных в осуществлении трудовой деятельности, проведения лечебно-профилактических мероприятий, оказания медицинской помощи, учета результатов исполнения договорных обязательств, повышения качества деятельности Учреждения, а также наиболее полного исполнения Учреждением обязательств и компетенций в соответствии с «Основами законодательства Российской Федерации об охране здоровья граждан» (ст. 61), законом «О медицинском страховании граждан в Российской

Федерации» (ст. 12), а также требованиями Трудового кодекса РФ (ст. 85-90), нормативно-методическими и распорядительными документами по организации ведения федерального регистра медицинских и фармацевтических работников, ведению кадрового и бухгалтерского учета (для работников Учреждения), Уставом Учреждения.

5.2. При определении объема и содержания обрабатываемых персональных данных Учреждение и его сотрудники должны руководствоваться федеральными законами и иными нормативными актами, устанавливающими цель обработки, а также определяющими требования по обеспечению безопасности персональных данных.

5.3. Персональные данные следует получать у самого субъекта персональных данных. При этом субъект дает согласие на использование своих персональных данных в письменном виде Приложение 3.

5.4. Согласие на обработку не требуется получать в случаях, если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных, обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности (например, штатный фотограф, штатный корреспондент) при условии, что при этом не нарушаются права и свободы субъекта персональных данных (ФЗ-152 «О персональных данных», ст.6, п.2).

5.5. Если персональные данные получаются у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее. Оператор должен сообщить субъекту наименование и адрес оператора или его представителя, цель обработки персональных данных и ее правовое основание, предполагаемых пользователей персональных данных, установленные Федеральным законом «О персональных данных» права субъекта персональных данных (ФЗ-152 «О персональных данных», гл. 4, ст. 18, п.3).

5.6. Оператор не имеет права получать и обрабатывать персональные данные субъектов персональных данных о его членстве в общественных объединениях или его профсоюзной деятельности, политических, религиозных и иных убеждениях и частной жизни (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений). В случаях, непосредственно связанных с вопросами трудовых отношений субъекта указанные в данном пункте сведения могут быть получены и обработаны оператором только с письменного согласия субъекта.

5.7. Все меры конфиденциальности при обработке персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

5.8. Не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу, лицу его замещающему, работникам отдела кадров и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки, без согласия субъекта и уведомления его о юридических последствиях такой обработки.

5.10. Типовые формы документов (в том числе договоров), предполагающих содержание персональных данных, должны согласовываться с юридическим отделом, который проверяет их на соответствие нормативно-правовым актам о персональных данных.

5.11. Должностным лицам запрещается заранее ставить на чистых бланках документов подпись и печать.

5.12. Запрещается использование обратной стороны бумажных носителей персональных данных для черновиков.

5.13. На рабочем столе работника должен находиться только тот массив документов, с которым в настоящий момент он работает. Другие документы, дела, журналы должны находиться в запертом шкафу.

5.14. Исполняемые документы не разрешается хранить в россыпи. Их следует помещать в папки, на которых указывается вид производимых с ними действий, например: для подшивки в личные дела, для отправки и т.п., или фамилии граждан, к работе с которыми относятся данные документы.

5.15. В конце рабочего дня все носители, содержащие персональные данные (документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы) должны быть убраны в металлические шкафы, сейфы. Следует также проверить урну для бумаг и убедиться в отсутствии там листов бумаги, которые могут представлять интерес для постороннего лица.

Общие требования по организации безопасной работы в информационных системах персональных данных

6.1. Главный врач ГБУЗ РБ ГКБ № 13 г. Уфа назначает сотрудника, исполняющем обязанности администратора информационной безопасности (далее - администратор информационной безопасности).

6.2. Администратор информационной безопасности действует на основании приказа о назначении и инструкции администратора безопасности, утвержденной главным врачом ГБУЗ РБ ГКБ № 13 г. Уфа.

6.3. Руководителями структурных подразделений совместно с администратором информационной безопасности определяются технические средства защиты персональных данных, используемые в ИСПДн, перечень которых утверждается главным врачом Учреждения.

6.4. Работа администраторов, пользователей и обслуживающего технические и программные средства персонала с информационной системой персональных данных должна осуществляться в полном соответствии с требованиями

настоящего Положения, Инструкции пользователя ИСПДн, Инструкции администратора ИСПДн.

6.5. Антивирусный контроль осуществляется в соответствии с Инструкцией о применении средств антивирусной защиты информации ГБУЗ РБ ГКБ № 13 г. Уфа.

6.6. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Учреждения, допущенному к работе с конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в системе. Некоторым сотрудникам в случае производственной необходимости могут быть сопоставлены несколько уникальных имен (учетных записей).

6.7. Аутентификация пользователей осуществляется по паролю. Требования к парольной политике описаны в соответствующем разделе Политики информационной безопасности.

6.8. При взаимодействии с сетью Интернет должно обеспечиваться противодействие атакам хакеров и распространению спама.

6.9. Порядок подключения и использования ресурсов сети Интернет должен контролироваться подразделением (сотрудниками) Учреждения, ответственными за обеспечение информационной безопасности. Любое подключение и использование сети Интернет должно быть санкционировано руководством подразделения.

6.10. Необходимо ограничить использование сети Интернет с автоматизированных рабочих мест, которые входят в состав ИСПДн. Для выхода Интернет должны использоваться специально выделенные автоматизированные рабочие места, не входящие в состав ИСПДн.

6.11. Данные, хранящиеся в ИСПДн, необходимость в обработке которых пропала, передаются на хранение в архив с составлением акта передачи в архив и затем уничтожаются в ИСПДн. Для хранения, комплектования и использования этих данных в архиве создается автоматизированный

научно-справочный аппарат архива, представляющий собой комплекс электронных справочников (база данных описаний документов), предназначенных для эффективного поиска архивных документов и информации. («Основные правила работы архивов организаций», одобренные решением Коллегии Росархива от 06.02.2002, п. 7.7.1).

6.12. При окончательном уничтожении всех документов, дел, записей в базе данных, содержащих персональные данные, следует уведомить об этом субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, - также в указанный орган [ФЗ РФ №152, гл.4, ст. 21] (например, при уничтожении всех документов, дел, записей в базе данных, содержащих данные об окладе, о начислении заработной платы, о составе семьи и т.д.).

6.13. В информационных системах персональных данных должны использоваться только сертифицированные по требованиям безопасности информации технические средства и системы защиты.

6.14. Сотрудниками управления информатизации должны производиться регулярные обновления операционных систем, системных и прикладных программ, средств защиты информации, антивирусных баз, резервное копирование критичной информации ИСПДн.

6.15. Любые работы с кабельными системами (телефонными линиями, локальными вычислительными сетями, электросетью) должны проводиться с санкции начальника Отдела АСУ и согласовываться с администратором информационной безопасности. В разрешении на проведение работ должны быть указаны дата и сроки проведения технических работ.

Учет

7.1. В информационных системах персональных данных, либо средствах защиты информации должен быть обеспечен контроль вывода информации на

бумажные носители, контроль доступа к файлам ИСПДн, и контроль копирования файлов на отчуждаемые носители.

7.2. Электронные отчуждаемые носители персональных данных (флэш-накопители, дискеты, оптические накопители и т.п.) подлежат учету в журнале учета отчуждаемых электронных носителей. Форма журнала приведена в Приложение . Журнал хранится в Отделе АСУ у ответственного лица, назначаемого приказом главного врача Учреждения. Сдаваемые электронные отчуждаемые носители персональных данных многократного пользования должны быть подвергнуты ответственным лицом процедуре уничтожения остаточной информации и храниться в сейфе до необходимости повторной выдачи. Запрещается использовать для переноса персональных данных неучтенные электронные носители.

7.3. Входящие документы регистрируются в Канцелярии.

7.4. Все документы, передаваемые во внешние организации, должны регистрироваться в Канцелярии как исходящие и иметь бумажные или электронные копии, хранящиеся в Канцелярии или в подразделениях, которые разрабатывают эти документы.

7.5. Выдача персонифицированных документов (в том числе справки, расчетные листки) производится лично лицу, указанному в документе, при предъявлении паспорта под роспись в соответствующем журнале, либо по нотариально заверенной доверенности. При необходимости для каждого вида документов заводится отдельный журнал.

Хранение

8.1. Хранение персональных данных должно происходить в порядке, исключающем их утрату и/или их неправомерное использование.

8.2. Архивные дела, конфиденциальные документы, учетные журналы и книги учета хранятся в рабочее и нерабочее время в металлических запирающихся

шкафах, либо специально выделенных для хранения помещениях с регламентированным доступом (далее - хранилища).

8.3. Трудовые книжки и иные важные документы хранятся в металлическом шкафу, сейфе либо выделенном помещении с регламентированным доступом. К важным документам следует относить документы, утрата которых либо утечка содержащейся в них информации способна привести к негативным последствиям для субъекта персональных данных (например, данные о заработной плате).

8.4. Материалы, связанные с анкетированием, тестированием, проведением собеседований относятся к документам, содержащим персональные данные высокой степени конфиденциальности, и помещаются в отдельное дело.

8.5. При отзыве согласия субъекта персональных данных его данные передаются на архивное хранение в архив ГБУЗ РБ ГКБ № 13 г. Уфа. Организация хранения, комплектования, учета и использования содержащих архивных документов должна происходить в соответствии с законодательством об архивном деле в Российской Федерации.

8.6. В каждом подразделении, ведущем обработку персональных данных, должны быть назначены сотрудники, ответственные за хранение документов, содержащих персональные данные, а также должны быть выделены хранилища для хранения закрепленных за сотрудниками документов, дел.

8.7. Документы выдаются для работы в начале дня исполнителям сотрудником, ответственным за хранение документов и конце дня должны быть сданы и заперты в хранилище, которое должно опечатываться печатью ответственного за хранение документов в данном хранилище.

8.8. Оттиск печати проставляется на тонкий слой пластилина или специальной мастики таким образом, чтобы оттиск невозможно было снять и восстановить.

8.9. Ответственными за хранение следует назначать заведующего подразделением и его заместителя на время отсутствия начальника.

8.10. Ключи от металлических шкафов (сейфов) выдаются и сдаются заведующему подразделением в конце рабочего дня под роспись в соответствующем журнале, с проставлением даты и времени.

8.11. Печати, штампы, бланки документов, ключи от хранилищ хранятся только в металлическом шкафу (сейфе) заведующего подразделением.

Уничтожение

9.1. Уничтожение документов, содержащих персональные данные, производится по достижении целей их обработки.

9.2. Уничтожению подлежат документы, не подлежащие архивному хранению, а также не имеющие научно-исторической ценности или иного практического значения.

9.3. Для уничтожения документов, содержащих персональные данные, приказом главного врача создается экспертная комиссия в составе не менее трех человек. В нее могут входить заместители главного врача, заведующий Канцелярией, заведующий Архивом или ведущий специалист отдела.

9.4. Уничтожение производится после утверждения главным врачом заполненного акта по форме, указанной в Приложении 5.

9.5. Уничтожение производится по мере необходимости в зависимости от объемов, накопленных для уничтожения документов.

9.6. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные должны храниться в отдельном деле или другом контейнере, доступ к которому физически ограничен.

9.7. Копии и черновики документов, содержащих персональные данные по минованию надобности должны уничтожаться в специальной бумагорезальной машине (шредере).

9.8. Черновики, копии документов, документы, не подлежащие учету, разрешается уничтожать без составления акта и создания комиссии на шредере.

Передача

10.1. При передаче персональных данных субъекта оператор должен соблюдать следующие требования:

10.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

10.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

10.1.3. Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

10.1.4. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

10.1.5. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

10.1.6. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

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

10.3. Транспортировка, передача носителей персональных данных должна происходить в порядке, исключающем случайную утрату носителей или утечку персональных данных (например, папки, портфели, кейсы).

10.4. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу.

10.5. При передаче персональных данных работника необходимо соблюдать следующие требования [ТК РФ, гл. 14, ст. 88]:

10.5.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных федеральными законами.

10.5.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

10.5.3. Предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать их конфиденциальность.

10.5.4. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

10.6. На основании федерального законодательства персональные данные работника могут запрашиваться и передаваться в налоговые органы, органы статистики (в обезличенном виде), пенсионные фонды (Управление пенсионного фонда по РФ), военкоматы г. Уфы, в органы социальной защиты (Управление социальной защиты граждан по г. Уфа), в судебные (городской суд, районный суд, верховный суд, арбитражный суд, конституционный суд, мировой суд), правоохранительные (прокуратура, УВД, МВД) и другие органы в пределах их полномочий, при предъявлении их сотрудниками соответствующих документов.

10.7. Единоразовую передачу персональных данных граждан вышеозначенным государственным структурам следует проводить с разрешения главного врача, которое оформляется в виде приказа главного врача о передаче персональных данных конкретным сотрудникам вышеозначенных органов. Передача информации, либо ознакомление с ней фиксируется в соответствующем журнале.

10.8. Порядок передачи персональных данных между сотрудниками в пределах ГБУЗ РБ ГКБ № 13 г. Уфа:

10.8.1. Передача персональных данных может осуществляться только лицам, имеющим допуск к персональным данным.

10.8.2. Дела и документы выдаются под роспись в журнале учета. При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений, включения в дело других документов или подмены документов.

10.8.3. При смене работников, ответственных за учет и хранение документов, содержащих персональные данные, составляется в произвольной форме акт их приема-сдачи, который утверждается заведующим подразделения, которому принадлежат работники.

10.8.4. Работник, не имеющий допуска, имеет право знакомиться с документами, содержащими только его персональные данные (карточкой формы Т-2, трудовой книжкой, приказами и заявления, содержащими его персональные данные). Ознакомление с этими документами должно производиться таким образом, чтобы избежать их утраты.

10.9. Запрещается выносить документы, содержащие персональные данные работника, из служебных помещений для работы с ними на дому. В необходимых случаях главный врач может разрешить исполнителям или секретарю-референту вынос из здания таких документов для их согласования, подписи и т.п. в организациях, находящихся в пределах города.

10.10. Лицам, выезжающим на другие территории, запрещается иметь при себе в пути следования документы и машинные носители, содержащие персональные данные. Эти материалы должны быть направлены заранее по адресу организации по месту командировки сотрудника заказными или ценными почтовыми отправлениями.

10.11. При передаче персональных данных на обработку третьим лицам с ними должен заключаться договор, существенным условием которого является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке. [ФЗ РФ №152, гл.2, ст. 6, п. 4].

Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

11.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

11.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

11.3. Руководитель, разрешающий доступ сотрудника к конфиденциальным сведениям, несет персональную ответственность за данное разрешение.

11.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

11.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

11.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не

предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

11.5.3. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет наложение на граждан или должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

11.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

11.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

11.7. Лица, ответственные за реализацию системы защиты информации, несут ответственность за достаточность и эффективность применяемых организационных и технических мер.

11.8. Каждый сотрудник, работающий в помещениях с персональными данными, несет персональную ответственность за исключение НСД к носителю и конфиденциальность содержащейся на нем информации.

11.9. Лица, работающие с персональными данными, а также пользователи (ответственные пользователи криптосредств), несут ответственность за несоблюдение ими требований документов, регламентирующих организацию и обеспечение безопасности персональных данных при их обработке, в соответствии с законодательством Российской Федерации.

Приложение 1

Гл. врачу ГБУЗ РБ ГКБ № 13 г. Уфа

_____

от _____
(должность начальника отдела)

_____

_____

(фамилия, имя, отчество)

ПРЕДСТАВЛЕНИЕ

на предоставление допуска к персональным данным

Прошу предоставить сотрудникам_____
(подразделение)
допуск к персональным данным, обрабатываемым в ГБУЗ РБ ГКБ № 13 г. Уфа, в связи с исполнением ими своих должностных обязанностей в соответствии со следующим перечнем:

ФИО сотрудника	Отдел, должность	Персональные данные, к которым необходимо предоставить допуск[1]

_____
(дата)

_____
(подпись)

[1] При предоставлении допуска руководствоваться принципом минимизации полномочий, т.е. выдавать допуск к тем массивам документов, которые действительно требуются для исполнения обязанностей сотрудника. Выдавать допуск ко всем документам, обрабатываемым в отделе «Наименование отдела» разрешается, но не рекомендуется.

Приложение 2

ОБЯЗАТЕЛЬСТВО

о неразглашении персональных данных, обрабатываемых в ГБУЗ РБ ГКБ № 13 г. Уфа

Я, _____,
(фамилия, имя, отчество)

в период трудовых отношений с ГБУЗ РБ ГКБ № 13 г. Уфа и в течение *5 (пяти) лет* после их окончания в соответствии с Положением о защите персональных данных пациентов и работников ГБУЗ РБ ГКБ № 13 г. Уфа обязуюсь:

1) не разглашать и не передавать третьим лицам, сведения, содержащие персональные данные, которые будут мне доверены или станут известны по работе, кроме случаев, предусмотренных законодательством Российской Федерации и с разрешения главного врача ГБУЗ РБ ГКБ № 13 г. Уфа;

2) выполнять относящиеся ко мне требования приказов, инструкций и положений по работе с персональными данными, действующих в ГБУЗ РБ ГКБ № 13 г. Уфа;

3) в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, немедленно сообщить об этом специалисту по обеспечению безопасности информации в ключевых системах информационной инфраструктуры или главному врачу ГБУЗ РБ ГКБ № 13 г. Уфа;

4) не производить преднамеренных действий, нарушающих достоверность, целостность, доступность и/или конфиденциальность персональных данных, хранимых и обрабатываемых с использованием информационных систем персональных данных ГБУЗ РБ ГКБ № 13 г. Уфа, либо без их использования.

5) в случае увольнения обязуюсь незамедлительно передать ГБУЗ РБ ГКБ № 13 г. Уфа все носители, содержащие персональные данные, полученные во время работы.

До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности персональных данных, обрабатываемых в ГБУЗ РБ ГКБ № 13 г. Уфа. Мне известно, что нарушение этого обязательства может повлечь гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

С Положением по организации и проведению работ по обеспечению безопасности персональных данных ознакомлен.

Проинструктировал:

_____ _____ _____
(должность) (подпись) (ФИО)

_____ «___»_____ _____г.

Обязательство принял:

_____ _____ _____
(должность) (подпись) (ФИО)

_____ «___»_____ _____г.

Приложение 3

Согласие на обработку персональных данных

Я, нижеподписавшийся (аяся),_____
(Фамилия, имя, отчество)

проживающий (ая) по адресу: _____
паспорт серии _____ № _____ выдан _____
(дата, наименование выдавшего органа)

в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 г. №152-ФЗ «О персональных данных», подтверждаю свое согласие на обработку (далее - Оператор) моих персональных данных, персональных данных моего/ей сына (дочери, подопечного) _____
(Ф.И.О. сына, дочери, подопечного)

включающих: фамилию, имя, отчество, пол, дату рождения, адрес проживания, контактный телефон, паспортные данные, реквизиты полиса ОМС, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью - в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания мне Оператором медицинской помощи я предоставляю право передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам, в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов) по ОМС. Оператор имеет право во исполнение своих обязательств по работе в системе ОМС на обмен (прием и передачу) моими персональными данными со страховой медицинской организацией _____
и территориальным фондом ОМС с использованием цифровых носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будут осуществляться лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет для стационара и пять лет для поликлиники.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной «_____» _____ 201___ года и действует бессрочно.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

Контактный телефон _____
Адрес по месту регистрации_____
_____

Подпись субъекта персональных данных _____

Приложение 4

ЖУРНАЛ

учета электронных отчуждаемых носителей персональных данных наименование структурного подразделения

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.
На _____листах

_____ _____
Должность и ФИО ответственного за хранение Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*
1						
2						
3						
4						
5						

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 5

УТВЕРЖДАЮ

_____

_____
(подпись)

«__» _____ 20__г.

Акт
об уничтожении персональных данных

Комиссия в составе:
Председатель – _____

Члены комиссии – _____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации, записанная на них в процессе эксплуатации информация, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем
_____.
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ /_____/

Члены комиссии: _____ /_____/
_____ /_____/