«СОГЛАСОВАНО»
ПРЕДСЕДАТЕЛЬ ПРОФКОМА
ОБУЗ «ГКБ №4»

_____ Т.Н. Батыгина
_____ 201 4 г.

«УТВЕРЖДАЮ»
ГЛАВНЫЙ ВРАЧ
ОБУЗ «ГКБ №4»

_____ А.В. Кукушкин
_____ 201 4 г.

Положение
о порядке обработки персональных данных работников
Областного бюджетного учреждения здравоохранения «Городская клиническая больница №4»
и гарантии их защиты

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет порядок обработки персональных данных работников и разработано в целях защиты персональных данных работников ОБУЗ «ГКБ №4» от несанкционированного доступа и порядка обработки.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, Федерального закона №149-ФЗ «Об информации, информатизации и защите информации» и Федерального закона № 152-ФЗ «О персональных данных».

1.3. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

1.4. Положение распространяется на отношения по обработке и защите персональных данных, полученных Оператором как до, так и после утверждения настоящего Положения, за исключением случаев, когда по причинам правового, организационного или иного характера Положение не может быть распространено на отношения по обработке и защите персональных данных, полученных до ее утверждения.

1.5. Сбор, хранение, использование и распространение информации о частной жизни лица без письменного его согласия не допускается. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

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

1.7. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.8. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

1.9. 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.

1.10. Настоящее Положение утверждается и вводится в действие приказом главного врача ОБУЗ «ГКБ №4» и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

II. ОСНОВНЫЕ ПОНЯТИЯ

2.1. Персональные данные работника – информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2 **Документы, содержащие персональные данные работника** - документы, которые работник предоставляет оператору (работодателю) в связи с трудовыми отношениями и касающиеся конкретного работника (субъекта персональных данных), а также другие документы, содержащие сведения, предназначенные для использования в служебных целях

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

2.4. **Конфиденциальная информация** – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.

2.5. **Разглашение конфиденциальной информации** - умышленное или неумышленное (неосторожное) действие лица, приведшие к ознакомлению (оглашению) с конфиденциальными сведениями лиц, не имеющих в установленном порядке допуска к конфиденциальным сведениям

2.6 **Оператор** – Областное бюджетное учреждение здравоохранения «Городская клиническая больница №4» (государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными).

2.7. **Обработка персональных данных работника** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.8. **Распространение персональных данных** - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц.

2.9. **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц.

2.10. **Блокирование персональных данных** - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.11. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников.

2.12. **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику.

III. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

3.1. В соответствии с Трудовым кодексом РФ, другими федеральными законами, локальными нормативными актами ОБУЗ «ГКБ №4» при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю следующие документы, содержащие персональные данные:

– паспорт или иной документ, удостоверяющий личность, содержащий сведения о паспортных данных работника, сведения о месте регистрации (месте жительства), сведения о семейном положении;

– трудовую книжку, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой, повреждением или по другим причинам;

– страховое свидетельство обязательного пенсионного страхования, содержащее сведения о номере и серии страхового свидетельства;

– свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;

– документы воинского учета - содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;

– документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащие сведения об образовании, профессии;

– сведения о предварительном (периодическом) медицинском осмотре (обследовании);

– справку, выданную органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с Трудовым кодексом РФ или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию);

– справку от нарколога;

– справку от психиатра.

3.2. В состав персональных данных работника входят:

– анкетные и биографические данные;

– образование;

– сведения о трудовом и общем стаже;

– сведения о составе семьи;

– паспортные данные;

– сведения о воинском учете;

– сведения о заработной плате сотрудника;

– сведения о социальных льготах;

– специальность,

– занимаемая должность;

– наличие судимостей;

– адрес места жительства;

– домашний телефон (мобильный телефон);

– место работы или учебы членов семьи и родственников;

– характер взаимоотношений в семье;

– содержание трудового договора;

– состав декларируемых сведений о наличии материальных ценностей;

– 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;

– результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

– фотографии и иные сведения, относящиеся к персональным данным работника;

– рекомендации, характеристики и т.п.;

– копии отчетов, направляемые в органы статистики.

3.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

IV. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Основной задачей обеспечения безопасности персональных данных при обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействии с целью хищения данных, разрушения (уничтожения) или искажении их в процессе обработки.

4.2. Для обеспечения безопасности персональных данных Организация руководствуется следующими принципами:

- законность: защита данных основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты персональных данных;
- системность: обработка данных в Организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых дни понимания и решения проблемы обеспечения безопасности данных;
- комплексность: защита персональных данных строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Организации и других имеющихся в Организации систем и средств защиты;
- непрерывность: защита данных обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки данных, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности персональных данных, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты данных осуществляется на основании результатов анализа практики обработки данных в Организации с учетом выявления новых способов и средств реализаций угроз безопасности данных, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности данных возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой персональных данных;
- минимизация прав доступа: доступ к данным предоставляется Работникам только в объеме, необходимом для выполнения их должностях обязанностей;
- гибкость: обеспечение выполнения функций защиты данных при изменении характеристик функционирования информационных систем персональных данных Организации, а также объема и состава обрабатываемых данных;
- специализация и профессионализм: реализация мер по обеспечению безопасности данных осуществляется Работниками, имеющими необходимые квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Организации предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности данных;
- наблюдаемость и прозрачность: меры по обеспечению безопасности данных должны быть спланированы так, чтобы результаты их применений были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты данных, а результаты контроля регулярно анализируются.

4.3. В Организации не производится обработка данных, несовместимая с целями сбора. Если иное не предусмотрено федеральным законом, по окончании обработки данных в Организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией данные уничтожаются или обезличиваются.

4.4. При обработке персональных данных обеспечивается их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных персональных данных.

V. СБОР И ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Источником информации обо всех персональных данных работника является непосредственно работник. Если персональные данные возможно получить только у третьей стороны, то работник должен быть заранее в письменной форме уведомлен об этом и от него должно быть получено письменное согласие. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

5.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

- Обработка персональных данных работника 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 работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов.
- При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами;
- Получение персональных данных о работнике может осуществляться как путем представления их самим работником, так и путем получения их из иных источников;
- Обработка персональных данных работников работодателем возможна только с их согласия. Исключения составляют случаи, предусмотренные законодательством РФ (в частности, согласие не требуется при наличии оснований, перечисленных в п. п. 2 - 11 ч. 1 ст. 6, п. п. 2 - 10 ч. 2 ст. 10, ч. 2 ст. 11 Федерального закона от 27.07.2006 N 152-ФЗ);
- Персональные данные следует получать у него самого. Если персональные данные работника, возможно, получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;
- Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия;
- Письменное согласие работника на обработку своих персональных данных должно включать в себя, в частности, сведения, указанные в п. п. 1 - 9 ч. 4 ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ;
- Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

5.3. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника должны соблюдать, в частности, следующие общие требования:

- При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами;

- При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- Защита персональных данных работника от неправомерного их использования, утраты обеспечивается работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ и иными федеральными законами;
- Работники и их представители должны быть ознакомлены под расписку с документами Компании, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области;
- Работники не должны отказываться от своих прав на сохранение и защиту тайны.

5.4. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

№	Роль	Цели и категории работников подразделений, которые обрабатываются	Должность работника
1	Осуществление контроля над обработкой персональных данных, обработка персональных данных	Обработка в рамках трудовых отношений; в рамках гражданско-правовых отношений; в целях выполнения и решения возложенных задач на ОБУЗ «ГКБ №4» в области здравоохранения в т.ч. врачебная тайна	Главный врач Заместитель главного врача по медицинской части Главная медицинская сестра
		Обработка в рамках трудовых отношений; в рамках гражданско-правовых отношений	Главный бухгалтер
		Обработка в рамках трудовых отношений	Начальник отдела кадров
2	Обработка персональных данных	Обработка в рамках трудовых отношений; в рамках гражданско-правовых отношений; в целях выполнения и решения возложенных обязанностей	Заместители главного врача; Главные специалисты подразделений ОБУЗ «ГКБ №4»; Работники планово-экономического отдела; Специалисты по охране труда; Работники юридического отдела и отдела закупок; Работники отдела кадров; Медицинский регистратор (архива)
3	Обработка персональных данных	Обработка в рамках трудовых отношений	Работники отдела кадров; Заведующие отделениями; Старшие медицинские сестры; Начальники отделений и служб;
4	Обработка персональных данных	Обработка в рамках трудовых отношений; в рамках гражданско-правовых отношений	Работники планово-экономического отдела; Работники бухгалтерии.

5.5. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

5.6. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

5.7. Обработка персональных данных работника не требует получения соответствующего согласия в следующих случаях:

– Если объем обрабатываемых работодателем персональных данных не превышает установленные перечни, а также соответствует целям обработки, предусмотренным трудовым законодательством, законодательством Российской Федерации о государственной гражданской службе;

– В случаях, предусмотренных коллективным договором, в том числе правилами внутреннего трудового распорядка, являющимися, как правило, приложением к коллективному договору, соглашением, а также локальными актами работодателя, принятыми в порядке, установленном ст. 372 Трудового кодекса РФ;

– Обязанность по обработке, в том числе опубликованию и размещению персональных данных работников в сети Интернет, предусмотрена законодательством Российской Федерации;

– Обработка персональных данных близких родственников работника в объеме, предусмотренном унифицированной формой № Т-2, утвержденной постановлением Госкомстата Российской Федерации от 05 мая 2004 г. № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством Российской Федерации (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат). В иных случаях, получение согласия близких родственников работника является обязательным условием обработки их персональных данных;

– Обработка специальных категорий персональных данных работника, в том числе, сведений о состоянии здоровья, относящихся к вопросу о возможности выполнения работником трудовой функции на основании положений п. 2.3 ч. 2 ст. 10 Федерального закона «О персональных данных» в рамках трудового законодательства;

– При передаче персональных данных работника третьим лицам в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

– При передаче его персональных данных в случаях, связанных с выполнением им должностных обязанностей, в том числе, при его командировании (в соответствии с Правилами оказания гостиничных услуг в Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 25 апреля 1997 г. № 490, нормативными правовыми актами в сфере транспортной безопасности);

– В случаях передачи работодателем персональных данных работников в налоговые органы, военные комиссариаты, профсоюзные органы, предусмотренные действующим законодательством Российской Федерации;

– При мотивированных запросах от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

Мотивированный запрос должен включать в себя указание цели запроса, ссылку на правовые основания запроса, в том числе подтверждающие полномочия органа, направившего запрос, а также перечень запрашиваемой информации.

В случае поступления запросов из организаций, не обладающих соответствующими полномочиями, работодатель обязан получить согласие работника на предоставление его персональных данных и предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, а также требовать от этих лиц подтверждения того, что это правило будет(было) соблюдено.

– Передача персональных данных работника кредитным организациям, открывающим и обслуживающим платежные карты для начисления заработной платы, осуществляется без его согласия в следующих случаях:

1. договор на выпуск банковской карты заключался напрямую с работником и в тексте, которого предусмотрены положения, предусматривающие передачу работодателем персональных данных работника
2. наличие у работодателя доверенности на представление интересов работника при заключении договора с кредитной организацией на выпуск банковской карты и ее последующем обслуживании;
3. соответствующая форма и система оплаты труда прописана в коллективном договоре (ст. 41 Трудового кодекса РФ).

– Обработка персональных данных работника при осуществлении пропускного режима на территорию служебных зданий и помещений работодателя, при условии, что организация пропускного режима осуществляется работодателем самостоятельно либо если указанная обработка соответствует порядку, предусмотренному коллективным договором, локальными актами работодателя, принятыми в соответствии со ст. 372 Трудового кодекса РФ;

При привлечении сторонних организаций для ведения кадрового и бухгалтерского учета работодатель обязан соблюдать требования, установленные ч. 3 ст. 6 Федерального закона «О персональных данных», в том числе, получить согласие работников на передачу их персональных данных.

5.8. Обработка персональных данных соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их персональных данных на период принятия работодателем решения о приеме либо отказе в приеме на работу. Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым данное лицо заключил соответствующий договор, а также при самостоятельном размещении соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц. При поступлении в адрес работодателя резюме, составленного в произвольной форме, при которой однозначно определить физическое лицо его направившее не представляется возможным, данное резюме подлежит уничтожению в день поступления. В случае отказа в приеме на работу сведения, предоставленные соискателем, должны быть уничтожены в течение 30 дней. Получение согласия также является обязательным условием при направлении работодателем запросов в иные организации, в том числе, по прежним местам работы, для уточнения или получения дополнительной информации о соискателе. Исключение составляют случаи заключения трудового договора с бывшим государственным или муниципальным служащим. В соответствии со ст. 64.1 Трудового кодекса Российской Федерации работодатель при заключении трудового договора с гражданами, замещавшими должности государственной или муниципальной службы, перечень которых устанавливается нормативными правовыми актами Российской Федерации, в течение двух лет после их увольнения с государственной или муниципальной службы обязан в десятидневный срок сообщать о заключении такого договора представителю нанимателя (работодателю) государственного или муниципального служащего по последнему месту его с службы в порядке, устанавливаемом нормативными правовыми актами Российской Федерации.

5.9. Ведение кадрового резерва трудовым законодательством не регламентировано. В этом случае, обработка персональных данных лиц, включенных в кадровый резерв, может осуществляться только с их согласия, за исключением случаев нахождения в кадровом резерве действующих сотрудников, в трудовом договоре которых определены соответствующие положения. Согласие на внесение соискателя в кадровый резерв организации оформляется либо в форме отдельного документа. Обязательным является условие ознакомления соискателя с условиями ведения кадрового резерва в организации, сроком хранения его персональных данных, а также порядком исключения его из кадрового резерва.

VI. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством

6.2. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- 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 Трудовым кодексом РФ или иными федеральными законами;
- Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия;
- Предупредить лиц, получивших персональные данные работника, 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 персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное правило не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом РФ и иными федеральными законами;
- Осуществлять передачу персональных данных работников в пределах организации в соответствии с настоящим Положением, с которым работники должны быть ознакомлены под подпись;
- Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции;
- Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции

6.3. Персональные данные работников обрабатываются и хранятся в отделе кадров.

6.4. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

6.5. При получении персональных данных не от работника (за исключением случаев, предусмотренных ч. 4 ст. 18 Федерального закона от 27.07.2006 N 152-ФЗ) работодатель до начала обработки таких персональных данных обязан предоставить работнику 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 Федеральным законом от 27.07.2006 N 152-ФЗ права субъекта персональных данных;
- источник получения персональных данных.

6.6. 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.

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

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

6.9. С работниками, ответственными за хранения персональных данных, а так же с работниками, владеющими персональными данными в силу своих должностных обязанностей,

заключаются Соглашения о неразглашении персональных данных работников (Приложение №1 к настоящему Положению). Экземпляр соглашения хранится в отделе кадров.

VII. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Порядок хранения документов, содержащих персональные данные работников, осуществлять в соответствии с:

– Правилами, устанавливающими порядок ведения и хранения трудовых книжек, а также порядок изготовления бланков трудовой книжки и обеспечения ими работодателей, утвержденными Постановлением Правительства РФ от 16 апреля 2003 г. № 225 «О трудовых книжках»;

– Унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными Постановлением Госкомстата России от 05 января 2004 г. №1;

– Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным Приказом Минкультуры России от 25 августа 2010 г. № 558.

7.2. Информация персонального характера работника хранится и обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

7.3. Обработка персональных данных работников организации-оператора осуществляется смешанным путем:

– неавтоматизированным способом обработки персональных данных;
– автоматизированным способом обработки персональных данных.

7.4. Персональные данные работников хранятся на бумажных носителях и в электронном виде.

7.5. Личные дела, трудовые книжки, а также документы, содержащие персональные данные работников, хранятся в отделе кадров. Ответственные лица за хранение документов, содержащих персональные данные работников, назначаются Приказом главного врача ОБУЗ «ГКБ №4».

7.6. Хранение оконченных производством документов, содержащих персональные данные работников, осуществляется в помещениях оператора, предназначенного для хранения отработанной документации. Ответственные лица за хранение оконченных производством документов, содержащих персональные данные работников, назначаются Приказом главного врача ОБУЗ «ГКБ №4».

7.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Хранение документов, содержащих персональные данные работников, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения, документы подлежат уничтожению в порядке, предусмотренном приказами по архивному делу.

7.8. Работодатель обеспечивает ограничение доступа к персональным данным работников лицам, не уполномоченным Федеральным законодательством, либо работодателем для получения соответствующих сведений.

7.9. Доступ к персональным данным работников без специального разрешения имеют только должностные лица работодателя, допущенные к работе с персональными данными работников в соответствии с настоящим Положением. Данным категориям работников в их должностные обязанности включается пункт об обязанности соблюдения требований по защите персональных данных.

Персональные данные работников в полном объеме выдаются только главному врачу ОБУЗ «ГКБ №4», заместителю главного врача по медицинской части, начальнику отдела кадров, главному бухгалтеру и главной медицинской сестре.

Иным должностным лицам работодателя, допущенным к работе с персональными данными работников, документы, содержащие персональные данные выдаются, в объеме, необходимом для выполнения своих должностных обязанностей.

Начальник отдела кадров - единственное должностное лицо, которое может формировать личные дела, снимать копии с документов, делать выписки, составлять аналитические справки, и изымать (заменять) документы, хранящиеся в личных делах работников. Передача данных прав и полномочий вышеуказанного лица иным должностным лицам работодателя без специально оформленного Приказа главного врача ОБУЗ «ГКБ №4» запрещается.

7.10. Помещения, в котором хранятся персональные данные работников, должны быть оборудованы надежными замками.

7.11. Помещения, в котором хранятся персональные данные работников, в рабочее время при отсутствии в них работников должны быть закрыты.

7.12. Проведение уборки помещений, в котором хранятся персональные данные работников (отдел кадров, бухгалтерия, архив), должно производиться в присутствии работников указанных структурных подразделений.

VIII. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКА

8.1. Право доступа к персональным данным работников имеют:

- Главный врач ОБУЗ «ГКБ №4»;
- Заместители главного врача;
- Главная медицинская сестра;
- Руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения);
- Руководитель нового структурного подразделения при переводе работника из одного структурного подразделения в другое;
- Сам работник, носитель данных;
- Сотрудники отдела кадров, бухгалтерии, архива;
- Сотрудники организации при выполнении ими своих служебных обязанностей;
- Другие сотрудники организации только с письменного согласия самого работника, носителя данных.

8.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется настоящим Положением.

8.3. В целях информационного обеспечения работодателем могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги, информационные стенды для потребителей услуг, оказываемых работодателем). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, адрес, иные персональные данные, предоставленные работником.

8.4. При обезличивании персональных данных согласие работника на включение персональных данных в общедоступные источники персональных данных не требуется.

8.5. Сведения о работнике могут быть исключены из общедоступных источников персональных данных по требованию самого работника, либо по решению суда или иных уполномоченных государственных органов.

8.6. 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;
- пенсионные фонды;

– подразделения муниципальных органов управления.

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

8.8. 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.

IX. УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Уничтожение документов (носителей), содержащих персональные данные, производится путем сожжения, дробления (измельчений). Для уничтожения бумажных документов допускается применение шредера.

9.2. Персональные данные на электронных носителях уничтожаются путем стирания или форматирования носителя.

9.3. Уничтожение производится комиссией. Факт уничтожения данных подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

X. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

10.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленников возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий вязи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически развивающийся 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 оператора.

10.1.1. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами ОБУЗ «ГКБ №4».

10.1.2. Для защиты персональных данных работников необходимо соблюдать ряд мер:

ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

строгое избирательное и обоснованное распределение документов и информации между работниками;

рациональное размещение рабочих мест работников, при которых исключалось бы бесконтрольное использование защищаемой информации;

знание работником требований нормативно-методических документов по защите информации и сохранении тайны;

наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

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

организация порядка уничтожения информации;

своевременное выявление нарушений требований разрешительной системы доступа работниками подразделения;

воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

не допускается выдача личных дел сотрудников на рабочие места руководителей.

10.1.3. Личные дела могут выдаваться на рабочие места только главному врачу и в исключительных случаях, по письменному разрешению главного врача, руководителю структурного подразделения.

10.1.4. Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который устанавливается начальником отдела кадров.

10.2. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

10.3. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности ОБУЗ «ГКБ №4», посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров, бухгалтерии.

10.4. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

порядок приема, учета и контроля деятельности посетителей;

технические средства охраны, сигнализации;

порядок охраны территории, зданий, помещений;

требования к защите информации при интервьюировании и собеседованиях.

10.5. Оператор при обработке персональных данных работников обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

10.6. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

10.7. Обеспечение безопасности персональных данных работников достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– учетом автоматизированных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10.4. Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона № 152 «О персональных данных».

10.5. Выбор средств защиты информации для системы защиты персональных данных осуществляется оператором в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона № 152 «О персональных данных».

10.6. Для обеспечения безопасности персональных данных работника при неавтоматизированной обработке предпринимаются следующие меры:

- Определяются места хранения персональных данных (согласно настоящему Положению);
- В кабинетах, где осуществляется хранение документов, содержащих персональные данные работников, имеются сейфы, шкафы, стеллажи, тумбы;
- Дополнительно кабинеты, где осуществляется хранение документов, содержащих персональные данные работников, оборудованы замками и системой пожарной сигнализации.
- Оператор использует услуги охраны.
- Все действия по неавтоматизированной обработке персональных данных работников осуществляются только должностными лицами, согласно Списку должностей, (Приложение № 2 к настоящему Положению), и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.
- При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы;
- При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

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

10.7.Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление). Персональные данные работников, содержащиеся на материальных носителях уничтожаются по Акту об уничтожении персональных данных. Эти правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

10.8.Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

10.9. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

10.10. Для обеспечения безопасности персональных данных работника при автоматизированной обработке предпринимаются следующие меры:

- Все действия при автоматизированной обработке персональных данных работников осуществляются только должностными лицами, согласно Списка должностей, (Приложение № 3 к настоящему Положению), и только в объеме, необходимом данным лицам для выполнения своей трудовой функции;
- Персональные компьютеры, имеющие доступ к базам хранения персональных данных работников, защищены паролями доступа. Пароли устанавливаются Администратором

информационной безопасности и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных работников на данном ПК;

- Иные меры, предусмотренные Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных;
- Обработка персональных данных осуществляется с соблюдением требований, предусмотренных Постановлением Правительства от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

10.11. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с приказами по архивному делу, или продлевается на основании заключения экспертной комиссии оператора, если иное не определено законодательством РФ.

XI. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА И РАБОТОДАТЕЛЯ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1 Работник обязан:

11.1.1. При приеме на работу предоставить работодателю свои полные и достоверные персональные данные.

11.1.2. Для своевременной и полной реализации своих трудовых, пенсионных и иных прав работник обязуется поставить в известность работодателя об изменении персональных данных, обрабатываемых работодателем в связи с трудовыми отношениями, в том числе изменении фамилии, имени, отчества, паспортных данных, о получении образования, квалификации, получении инвалидности и иных медицинских заключений, препятствующих выполнению своих должностных обязанностей, и прочих данных с предоставлением подтверждающих документов**.**

11.2. В целях обеспечения защиты персональных данных работник имеет право на:

11.2.1 Полную информацию о хранящихся у работодателя его персональных данных.

11.2.2 Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством РФ.

Выдача документов, содержащих персональные данные работников, осуществляется в соответствии со ст. 62 Трудового кодекса Российской Федерации, гл. 3 ст. 14 Федерального закона № 152-ФЗ с соблюдением следующей процедуры:

- заявление работника о выдаче того или иного документа на имя главного врача ОБУЗ «ГКБ №4»;

- выдача заверенной копии (в количестве экземпляров, необходимом работнику) заявленного документа либо справки о заявленном документе или сведениях, содержащихся в нем;

- внесение соответствующих записей в журнал учета выданной информации.

11.2.3 Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

11.2.4 Требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.

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

11.2.6. Если работник считает, что работодатель осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его

права и свободы, работник вправе обжаловать действия или бездействие работодателя 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.

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

11.2.8. Иные права, предусмотренные действующим законодательством

11.3. Работодатель обязан:

11.3.1 Предоставить работнику, по его просьбе информацию о наличии у него персональных данных владельца, цели их обработки, способ обработки, разъяснить юридические последствия отказа работника от их предоставления в случае, если такая обязанность предусмотрена Федеральным законодательством.

11.3.2 По письменному заявлению работника не позднее 3-х рабочих дней со дня его подачи бесплатно выдавать работнику копии документов, связанных с работой.

11.3.3 Устранять выявленные недостоверные персональные данные в случаях и порядке, предусмотренном Федеральным законодательством.

11.3.4 Принимать возможные меры по обеспечению безопасности персональных данных работников при их обработке.

11.4. Работодатель имеет право:

11.4.1 Требовать от работника предоставления персональных данных и документов, их подтверждающих, в случаях, предусмотренных Федеральным законодательством.

11.4.2 Иные права, предусмотренные действующим законодательством.

XII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА

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

12.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

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

12.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут в соответствии с федеральными законами ответственность:

дисциплинарную (замечание, выговор, увольнение);

административную (предупреждение или административный штраф);

гражданско-правовую (возмещение причиненного убытка).

12.4. Работник, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, несет дисциплинарную ответственность, вплоть до увольнения.

XIII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1 Настоящее Положение утверждается и вводится в действие Приказом главного врача ОБУЗ «ГКБ №4».

13.2 Настоящее Положение вступает в силу с даты его утверждения, является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

13.3 В обязанности работодателя входит ознакомление всех работников с настоящим Положением и лиц, принимаемых на работу до подписания трудового договора, под личную подпись.

13.4. Главный врач ОБУЗ «ГКБ №4» вправе вносить изменения и дополнения в настоящее Положение. Работники ОБУЗ «ГКБ №4» должны быть поставлены в известность о вносимых изменениях и дополнениях посредством издания приказа главным врачом и ознакомления с ними всех работников ОБУЗ «ГКБ №4».

Приложение №1 к Положению «О порядке обработки персональных данных работников Областного бюджетного учреждения здравоохранения «Городская клиническая больница №4» и гарантии их защиты»

Соглашение о неразглашении персональных данных сотрудника

Я,_____, паспорт серии._____, номер _____ выданный _____ " ____" _____года,

понимаю, что получаю доступ к персональным данным сотрудников ОБУЗ «ГКБ №4». Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных сотрудников.

Я понимаю, что разглашение такого рода информации может нанести ущерб сотрудникам ОБУЗ «ГКБ №4» как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сборе, обработке и хранении) с персональными данными сотрудника соблюдать все описанные в "Положении о порядке обработки персональных данных работников ОБУЗ «ГКБ №4» и гарантии их защиты" требования.

Я подтверждаю, что не имею права разглашать сведения о (об):
анкетных и биографических данных;
образовании;
трудовом и общем стаже;
составе семьи;
паспортных данных;
воинском учете;
заработной плате сотрудника;
социальных льготах;
специальности;
занимаемой должности;
наличии судимостей;
адресе места жительства, домашнем телефоне;
месте работы или учебы членов семьи и родственников;
характере взаимоотношений в семье;
содержании трудового договора;
составе декларируемых сведений о наличии материальных ценностей;
содержании декларации, подаваемой в налоговую инспекцию;
подлинниках и копиях приказов по личному составу;
личных делах и трудовых книжках сотрудников;
делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
копиях отчетов, направляемых в органы статистики.
Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудника или их утраты, я несу ответственность в соответствии с ТК РФ.
С "Положением о порядке обработки персональных данных работников ОБУЗ «ГКБ №4» и гарантии их защиты" ознакомлен (а).

_____ _____ «__» _____ 20__г.

(должность) (Ф.И.О.) _____подпись

Приложение №2 к Положению «О порядке обработки персональных данных работников Областного бюджетного учреждения здравоохранения «Городская клиническая больница №4» и гарантии их защиты»

Список должностей работников ОБУЗ «ГКБ №4» уполномоченных на неавтоматизированную обработку персональных данных работников

1. **Главный врач;**
2. **Заместители главного врача;**
3. **Начальник отдела кадров;**
4. **Главный бухгалтер;**
5. **Начальник юридического отдела и отдела закупок;**
6. **Главная медицинская сестра;**
7. **Заведующие структурными подразделениями;**
8. **Старшие медицинские сестры;**
9. **Ведущий юрисконсульт;**
10. **Работники отдела кадров;**
11. **Работники бухгалтерии;**
12. **Работники планово-экономического отдела;**
13. **Специалисты по охране труда.**

Приложение №3 к Положению «О порядке обработки персональных данных работников Областного бюджетного учреждения здравоохранения «Городская клиническая больница №4» и гарантии их защиты»

Список должностей работников ОБУЗ «ГКБ №4» уполномоченных на автоматизированную обработку персональных данных работников

1. **Главный врач;**
2. **Заместители главного врача;**
3. **Начальник отдела кадров;**
4. **Главный бухгалтер;**
5. **Начальник юридического отдела и отдела закупок;**
6. **Главная медицинская сестра;**
7. **Заведующие структурными подразделениями;**
8. **Старшие медицинские сестры;**
9. **Ведущий юрисконсульт;**
10. **Работники отдела кадров;**
11. **Работники бухгалтерии;**
12. **Работники планово-экономического отдела;**
13. **Специалисты по охране труда.**