Государственное бюджетное учреждение здравоохранения
Кемеровской области
«Прокопьевская районная больница»
(ГБУЗ КО «Прокопьевская РБ»)

ПРИКАЗ № 21/1

г. Прокопьевск «09» января 2017 года

Об организации работы по защите
конфиденциальной информации
и персональных данных

В целях организации работы по защите конфиденциальной информации и персональных данных в ГБУЗ КО «Прокопьевская РБ», в соответствии с Конституцией РФ, Трудовым кодексом РФ, Гражданским кодексом РФ, Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие:
1.1. Положение о защите персональных данных (Приложение № 1)

2. Секретарю-машинистке – Водяковой Валентине Григорьевне, ознакомить работников, допущенных к сведениям, содержащим конфиденциальную информацию и персональные данные, с настоящим приказом.

3. Контроль за исполнением приказа оставляю за собой.

Главный врач
ГБУЗ КО «Прокопьевская РБ» Н.К. Кочкина

Приложение № 1
К приказу
ГБУЗ КО «Прокопьевская РБ»
от «09»января_2017г №21/1

Положение о персональных данных ГБУЗ КО «Прокопьевская РБ»

1. Общие положения

1.1. Целью данного Положения является закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Кодексом РФ об административных правонарушениях, Гражданским кодексом РФ, Уголовным кодексом РФ, а также Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

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 утверждается и вводится в действие приказом Главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Под персональными данными работников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника, а также сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. Состав персональных данных работника:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- адрес;
- семейное положение;
- социальное положение;
- имущественное положение;

- сведения об образовании;
- сведения о профессии;
- сведения о доходах;
- сведения о состоянии здоровья;
- фотографии;
- пол;
- гражданство;
- серия и номер паспорта;
- дата выдачи паспорта;
- сведения об учреждении, выдавшем паспорт;
- номер телефона;
- адрес электронной почты;
- сведения о постановке на учет в налоговом органе;
- серия и номер полиса медицинского страхования;
- номер страхового свидетельства обязательного пенсионного страхования;
- сведения о воинском учете;
- сведения о социальных льготах;
- должность;
- сведения о трудовой деятельности;
- сведения о повышении квалификации, переподготовке и аттестации;
- сведения о судимости;
- место работы или учебы членов семьи;
- содержание трудового договора;
- содержание приказов по личному составу;
- основания к приказам по личному составу;
- сведения о награждении государственными наградами, присвоении почетных, воинских и специальных званий.

2.3. Указанные в п. 2.2 сведения являются конфиденциальными и не подлежат разглашению иначе как по основаниям, предусмотренным законодательством РФ.

3. Создание, обработка и хранение персональных данных работника

3.1. Создание персональных данных работника.

Документы, содержащие персональные данные работника, создаются путем:

а) копирования оригиналов (документ об образовании, свидетельство ИНН, пенсионное свидетельство и т.д.);

б) внесения сведений в учетные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, медицинское заключение).

3.2. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных

данных работника.

3.2.1. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов.

3.2.2. Обработка персональных данных работника осуществляется исключительно в целях: обеспечения соблюдения Конституции Российской Федерации, законов и иных нормативных правовых актов РФ, содействия субъектам персональных данных в трудоустройстве, продвижении по службе, обучении, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора.

3.2.3. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны. При получения персональных данных работника необходимо получить его письменное согласие на обработку персональных данных (приложение № 1)

3.2.4. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

В согласии работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:

а) о целях получения персональных данных;

б) о предполагаемых источниках и способах получения персональных данных;

в) о характере подлежащих получению персональных данных;

г) о последствиях отказа работника дать письменное согласие на их получение.

3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.2.6. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.2.7. Работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

3.3. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы N Т-2, а также содержатся на

электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях.

3.4. Хранение персональных данных:

3.4.1. персональные данные, содержащиеся на бумажных носителях хранятся в соответствии с Инструкцией по организации работы с материальными носителями конфиденциальной информации утвержденной приказом;

3.4.2. персональные данные, содержащиеся на электронных носителях информации, хранятся в соответствии с Инструкцией по организации работы с электронными носителями конфиденциальной информации и персональных данных. утвержденной приказом.

3.4.3. Персональные данные, включенные в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте начальника отдела кадров.

3.4.4. Трудовая книжка, документы воинского учета, карточка формы N Т-2 хранятся в запертом металлическом сейфе в кабинете начальника отдела кадров.

3.4.3. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника имеют:

- главный врач учреждения;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
- сам работник, носитель данных;
- другие сотрудники организации, при выполнении ими своих служебных обязанностей, при начислении и выплате заработной платы, подготовке к аттестации рабочих мест, сдаче налоговых деклараций, подаче статистических данных.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом главного врача учреждения.

4.2. Внешний доступ.

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

- налоговые инспекции;
- правоохранительные органы;

- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;

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

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

4.2.4. Другие организации.

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

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

5. Защита персональных данных

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

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

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

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. Внутренняя защита.

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с

документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами учреждения.

5.5.2. Для обеспечения внутренней 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 котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранению 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 нарушения 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. Личные дела могут выдаваться на рабочие места только главному врачу, работникам отдела кадров и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается начальнику отдела кадров и программисту

5.6. Внешняя защита.

5.6.1. 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.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, 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.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников в соответствии с приложением № 2 к Положению.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными работника

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

6.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение № 1
к Положению о защите
персональных данных

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество)
паспорт серия _____ № _____, выдан _____
(кем и когда выдан)

Выражаю свое согласие свободно, своей волей и в своем интересе Государственному бюджетному учреждению здравоохранения Кемеровской области «Прокопьевская районная больница», расположенному по адресу: Кемеровская область, г. Прокопьевск, ул. Образцовая 11.,(в дальнейшем – Работодатель) на обработку следующих персональных данных:

- фамилия, имя, отчество;
- год рождения;
- месяц рождения;
- дата рождения;
- место рождения;
- адрес;
- семейное положение;
- социальное положение;
- имущественное положение;
- сведения об образовании;
- сведения о профессии;
- сведения о доходах;
- сведения о состоянии здоровья;
- фотографии;
- пол;
- гражданство;
- серия и номер паспорта;
- дата выдачи паспорта;
- сведения об учреждении, выдавшем паспорт;
- номер телефона;
- адрес электронной почты;
- сведения о постановке на учет в налоговом органе;
- серия и номер полиса медицинского страхования;
- номер страхового свидетельства обязательного пенсионного страхования;
- сведения о воинском учете;
- сведения о социальных льготах;
- должность;
- сведения о трудовой деятельности;
- сведения о повышении квалификации, переподготовке и аттестации;
- сведения о судимости;
- место работы или учебы членов семьи;
- содержание трудового договора;
- содержание приказов по личному составу;
- основания к приказам по личному составу;
- сведения о награждении государственными наградами, присвоении почетных,

воинских и специальных званий.

Обработка моих персональных данных допускается в следующих целях:

- оформления трудовых отношений;
- обеспечения сохранности имущества Работодателя;
- осуществления мною трудовой функции и оплаты моего труда;
- предоставления гарантий и льгот, предусмотренных нормативными правовыми актами, содержащими нормы трудового права, коллективным договором, соглашениями, локальными нормативными актами, трудовым договором;
- _____

Мои персональные данные могут обрабатываться следующими способами:

- автоматизированная обработка
- неавтоматизированная обработка
- _____

Я разрешаю осуществление следующих действий с моими персональными данными (нужное подчеркнуть)

- получение _____
(указать от кого (источник))
- передача _____
(указать кому)
- использование
- распространение
- хранение
- комбинирование

Срок действия согласия (нужное подчеркнуть или указать):

- на весь срок действия трудового договора и в течение одного года после окончания трудового договора.

Данное мною согласие может быть отозвано мною в любой момент с обязательным направлением Работодателю письменного уведомления. С момента получения уведомления об отзыве согласия на обработку персональных данных, а также при прекращении трудового договора Работодатель обязан прекратить обработку персональных данных и (или) уничтожить персональные данные в срок _____
(указать срок)
с даты получения такого отзыва.

Мне разъяснено, что при отзыве мною согласия Работодатель (или уполномоченный им оператор) вправе продолжить обработку моих персональных данных в случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

При достижении целей обработки мои персональные данные подлежат уничтожению в срок _____ с даты достижения таких целей с обязательным уведомлением в течение _____

Требование об уничтожении не распространяется на персональные данные, для которых нормативными правовыми актами предусмотрена обязанность их хранения, в том числе после прекращения трудовых отношений.

_____

Дата *Личная подпись* Расшифровка подписи

Приложение 2
к Положению о защите
персональных данных

Обязательство о неразглашении сведений конфиденциального характера и персональных данных

Я,_____
(фамилия, имя отчество)

сотрудник Государственного бюджетного учреждения здравоохранения Кемеровской области «Прокопьевская районная больница», расположенного по адресу: Кемеровская область, г. Прокопьевск, ул. Образцовая 11. (далее – Учреждение) обязанностей понимаю, что в период исполнения должностных обязанностей получаю доступ к персональным данным обрабатываемых в ГБУЗ КО «Прокопьевская РБ».

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке, накоплении, хранении и т.д.) с персональными данными физических лиц соблюдать все описанные в Федеральном законе от 27.07.2006 г. № 152-ФЗ «О персональных данных», постановлении Правительства РФ от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и других нормативных актах, требования.

1. Я подтверждаю, что не имею права разглашать сведения:
   - фамилия, имя, отчество;
   - год рождения;
   - месяц рождения;
   - дата рождения;
   - место рождения;
   - адрес;
   - семейное положение;
   - социальное положение;
   - имущественное положение;
   - сведения об образовании;
   - сведения о профессии;
   - сведения о доходах;
   - сведения о состоянии здоровья;
   - фотографии;
   - пол;
   - гражданство;
   - серия и номер паспорта;
   - дата выдачи паспорта;
   - сведения об учреждении, выдавшем паспорт;
   - номер телефона;
   - адрес электронной почты;
   - сведения о постановке на учет в налоговом органе;
   - серия и номер полиса медицинского страхования;
   - номер страхового свидетельства обязательного пенсионного страхования;
   - сведения о воинском учете;
   - сведения о социальных льготах;
   - должность;

- сведения о трудовой деятельности;
- сведения о повышении квалификации, переподготовке и аттестации;
- сведения о судимости;
- место работы или учебы членов семьи;
- содержание трудового договора;
- содержание приказов по личному составу;
- основания к приказам по личному составу;

сведения о награждении государственными наградами, присвоении почетных, воинских и специальных званий.

2. Учитывать, что все документы, подготовленные мною или совместно с другими сотрудниками Учреждения в рамках исследования каких-либо проблем и при использовании информационных, технических или других ресурсов ГБУЗ КО «Прокопьевская РБ», являются собственностью Учреждения.
3. Не разглашать персональные данные, которые мне будут доверены или станут известны при выполнении мной должностных обязанностей; а так же в результате технических сбоев в работе информационных систем Учреждения, или нарушения коллегами правил обработки персональных данных и получения мной несанкционированного доступа к персональным данным.
4. Не передавать третьим лицам и не раскрывать публично персональные данные, содержащиеся в информационных системах Учреждения без письменного распоряжения на выполнение таких действий руководителя Учреждения.
5. Строго выполнять относящиеся ко мне требования приказов, регламентов, правил, инструкций и положений, касающихся обработки персональных данных.
6. В случае моего увольнения, все носители персональных данных (черновики, таблицы, магнитные и оптические носители, дискеты, flash-накопители, распечатки на принтерах, и пр.), которые находились в моём распоряжении в связи с выполнением мною служебных обязанностей во время работы в Учреждении передать лично руководителю Учреждения или руководителю структурного подразделения в котором я непосредственно работал(а).
7. Об утрате носителей персональных данных, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), и о других фактах, которые могут привести к нарушению правил обработки персональных данных немедленно сообщать работнику (администратору информационной безопасности), ответственному за комплекс мероприятий по защите персональных данных, или лично руководителю Учреждения.
8. Знакомиться только с той информацией, которая необходима мне для выполнения своих должностных обязанностей.
9. О попытках выведывания, предложениях или угрозах, связанных с разглашением сведений ограниченного распространения, немедленно сообщать своему руководителю.
10. Немедленно доводить до сведения руководства известные мне факты разглашения или создания предпосылок к разглашению сведений ограниченного распространения.

Я на период моей работы в Учреждении, предоставляю ему право при необходимости проверять соблюдение мной требований положения по обеспечению сохранности сведений ограниченного распространения и иных требований безопасности методами, разрешенными законами Российской Федерации.

Мне известно, что нарушение этих положений может повлечь уголовную, административную, гражданско-правовую или иную ответственность, предусмотренную действующим законодательством Российской Федерации, в виде лишения свободы, увольнения, выговора, денежного штрафа, обязанности по возмещению ущерба учреждению (убытков, утраты деловой репутации и морального ущерба) и других наказаний.

С «Инструкцией по организации работы с материальными носителями персональных данных», «Инструкцией по организации работы с электронными носителями

персональных данных и другой конфиденциальной информации», утвержденными приказом № ___от_____, «Положением о защите персональных данных», утвержденным приказом №____от _____ в Учреждении ознакомлен(а).

Обязательство исполняется в двух экземплярах. После подписания один экземпляр обязательства вручается сотруднику, второй хранится в его личном деле.

« » _____201_г. _____/_____
Ф.И.О. подпись

ГБУЗ КО Прокопьевская РБ» подтверждает, что данные вами обязательства получены на добровольной основе, без принуждения и недопонимания сути данных обязательств.

«__» _____201_г. _____/_____
Ф.И.О. подпись

Один экземпляр обязательств получил

«__» _____201_г. _____/_____
Ф.И.О. подпись

Приложение №2 к приказу
ГБУЗ КО «Прокопьевская РБ»

Ответственные лица по работе с персональными данными работников

наименование должности	Ф.И.О.
Начальник отдела кадров	Шефер Екатерина Андреевна
Специалист отдела кадров	Борис Анна Игоревна
Заместитель главного бухгалтера	Киселева Жанна Анатольевна
Бухгалтер	Воробьева Светлана Александровна
Бухгалтер	Пархомук Наталья Сергеевна
Бухгалтер	Най Оксана Владимировна