Приложение 2
к приказу главного врача
от 03.04.15 № 171

УТВЕРЖДАЮ:
Главный врач КГБУЗ «КМКБ № 4»
_____ А. П. ФОКИНА
«03» 04 2015г.

# ПОЛОЖЕНИЕ
## о хранении и использовании персональных данных пациентов краевого государственного бюджетного учреждение здравоохранения «Красноярская межрайонная клиническая больница № 4»

### 1. Общие положения

1.1. Настоящим Положением определяется порядок обращения с персональными данными пациентов краевого государственного бюджетного учреждение здравоохранения «Красноярская межрайонная клиническая больница № 4» (далее - Организация).

1.2. Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав и интересов Организации и ее пациентов в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих (см. далее) персональные данные.

1.3. Персональные данные пациента - любая информация, относящаяся к данному пациенту (субъекту персональных данных) и необходимая Организации в связи с лечебно-профилактическими действиями, в том числе:

фамилия, имя, отчество пациента;

дата и место рождения пациента;

адрес пациента;

семейное, социальное положение пациента;

образование, профессия пациента;

другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных.

1.4. Сведения о персональных данных пациентов относятся к числу конфиденциальных (составляющих охраняемую законом тайну Организации). Режим конфиденциальности в отношении персональных данных снимается:

в случае их обезличивания (см. далее);

по истечении 25 лет (истории болезни) срока их хранения;

в других случаях, предусмотренных федеральными законами.

### 2. Основные понятия. Состав персональных данных Пациентов.

2.1. Для целей настоящего Положения используются следующие понятия:

персональные данные пациента - в соответствии с определением п. 1.3 настоящего Положения;

обработка персональных данных пациента - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в

том числе передача), обезличивание, блокирование, уничтожение персональных данных;

конфиденциальность персональных данных - обязательное для соблюдения назначенного ответственных лиц, получивших доступ к персональным данным пациентов, требование не допускать их распространения без согласия пациента или иного законного основания;

распространение персональных данных - действия, направленные на передачу персональных данных пациентов определенному кругу лиц (передача персональных данных) или ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных пациентов в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или представление доступа к персональным данным пациентов каким-либо иным способом;

использование персональных данных - действия (операции) с персональными данными, совершаемые уполномоченными должностными лицами Организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении пациентов либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных пациентов, в том числе их передачи;

уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных пациентов или в результате которых уничтожаются материальные носители персональных данных пациентов;

обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному пациенту;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия пациента, или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

информация - сведения (сообщения, данные) независимо от формы их представления;

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

2.2. Информация, представляемая пациентом при поступлении на лечение в Организацию, должна иметь документальную форму. При обращении в Организацию пациент предъявляет:

- паспорт или иной документ, удостоверяющий личность;
- страховое свидетельство медицинского страхования.

2.3. При оформлении пациента регистратурой Консультативно-диагностического отделения (КДО) заводится "Медицинская карта амбулаторного больного" (учетная форма № 025/у-04), в которой отражаются следующие анкетные и биографические данные пациента:

- общие сведения (Ф.И.О., дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о месте жительства и о контактных телефонах;

- сведения о заболеваниях.

Далее Карта заполняется медицинским работником (врачом-специалистом), осуществляющим наблюдения за больным. Все остальные записи в медицинской карте производятся лечащими врачами в установленном порядке, в порядке текущих наблюдений.

Здесь же записываются консультации специалистов, врачебных комиссий и т.д.

В случае госпитализации больного в стационар, оформляется карта стационарного больного. В случае смерти больного одновременно с выдачей врачебного свидетельства о смерти в карте производится запись о дате и причине смерти.

Медицинские карты умерших изымаются из действующей картотеки и передаются в архив лечебного учреждения, где хранятся 25 лет.

Медицинские карты амбулаторного больного хранятся в регистратуре. Медицинские карты стационарных больных хранятся в архиве.

## 3. Организация обработки персональных данных пациентов

3.1. Организация имеет права получать и обрабатывать персональные данные пациента о его состоянии здоровья, интимной жизни только с его письменного согласия (Согласие пациента на обработку его персональных данных).

3.2. Обработка указанных персональных данных пациентов Организацией возможна только с их согласия либо без их согласия в следующих случаях:

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

3.3. Письменное согласие пациента на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.
- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом.

3.4. Согласие пациента не требуется в следующих случаях:

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов сотрудника, если получение его согласия невозможно.

## 4. Передача персональных данных

4.1. При передаче персональных данных пациента Организация должна соблюдать следующие требования:

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

4.1.2. Осуществлять передачу персональных данных пациентов в пределах Организации в соответствии с настоящим Положением.

4.1.3. Разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.2. Персональные данные пациентов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети или через шифрованный канал интернет(VipNet).

## 5. Доступ к персональным данным пациентов

5.1. Право доступа к персональным данным пациент имеют:

- главный врач;
- сотрудники отделений стационара и подразделений КДО;
- сотрудники отдела статистики;
- сотрудники отдела АСУ.

5.2. Пациенты Организации имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные.

5.2.2. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия сотрудников Организации при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных пациента разрешается исключительно в служебных целях .

5.4. Передача информации третьей стороне возможна только при письменном согласии пациентов.

## 6. Ответственность за нарушение норм, регулирующих обработку персональных данных

6.1. Сотрудники Организации, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

Заместитель главного врача по
правовым и кадровым вопросам Н.М. Мамавко

Приложение 1
к Положению о хранении
и использовании персональных
данных пациентов

# СОГЛАСИЕ
## на обработку персональных данных

Я, нижеподписавшийся _____,
проживающий (ая) по адресу:_____,
паспорт_____,выдан_____,
дата выдачи _____ г., в соответствии с требованиями статьи 9 Федерального закона № 152-ФЗ от 27.07.2006 "О персональных данных", подтверждаю свое согласие на обработку КГБУЗ «Красноярская межрайонная клиническая больница № 4», 660094, г. Красноярск, ул. Кутузова, д. 71 (далее – Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес проживания, контактный телефон, реквизиты полиса ОМС (ДМС), 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 Оператором мне медицинской помощи я предоставляю право медицинским работникам, передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора, 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 (договором ДМС).

Оператор имеет право во исполнение своих обязательств по работе в системе ОМС (по договору ДМС.) на обмен (прием и передачу) моими персональными данными со страховой медицинской организацией и территориальным фондом ОМС с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будут осуществляется лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет (для стационара, 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 «_____»_____ 20_____ г. 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.

Подпись субъекта персональных данных _____

Приложение 1
к приказу главного врача
от 03.04.15 № 171

УТВЕРЖДАЮ:
Главный врач
КГБУЗ «КМКБ № 4»
_____А. П. ФОКИНА
«03» 04 2015г.

# ПОЛОЖЕНИЕ
## об обработке и защите персональных данных сотрудников краевого государственного бюджетного учреждения здравоохранения «Красноярская межрайонная клиническая больница № 4»

### 1. Общие положения

1.1. Настоящее Положение имеет своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни.

1.2. Настоящее Положение об обработке и защите персональных данных (далее - Положение) определяет порядок сбора, хранения, передачи и любого другого использования персональных данных работников, в соответствии с законодательством Российской Федерации и гарантии конфиденциальности сведений о работнике предоставленных работником работодателю.

1.3. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, 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", иными нормативно-правовыми актами, действующими на территории Российской Федерации.

### 2. Основные понятия

Для целей настоящего Положения используются следующие понятия:

2.1. Оператор персональных данных (далее 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. В рамках настоящего положения оператором является КГБУЗ «Красноярская межрайонная клиническая больница № 4» (далее -Учреждение).

2.2. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.

2.3. Субъект – субъект персональных данных.

2.4. Работник - физическое лицо, состоящее в трудовых отношениях с оператором.

2.5. 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.

2.6. 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.

2.7. 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.

2.8. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

2.9. 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.

2.10. К персональным данным относятся:

2.10.1. Сведения, содержащиеся в основном документе, удостоверяющем личность субъекта.

2.10.2. Информация, содержащаяся в трудовой книжке работника.

2.10.3. Информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования.

2.10.4. Сведения, содержащиеся в документах воинского учета для военнообязанных и лиц, подлежащих призыву на военную службу.

2.10.5. Сведения об образовании, квалификации или наличии специальных знаний или подготовки.

2.10.6. Сведения, содержащиеся в свидетельстве о постановке на учет физического лица в налоговом органе на территории Российской Федерации.

2.10.7. Сведения о семейном положении работника.

2.10.8. Информация медицинского характера, в случаях, предусмотренных законодательством.

2.10.9. Сведения о заработной плате работника.

2.10.10. Сведения о социальных льготах.

2.10.11. Сведения о наличии судимостей.

2.10.12. Место работы или учебы членов семьи.

2.10.13. Содержание трудового договора.

2.10.14. Подлинники и копии приказов по личному составу.

2.10.15. Основания к приказам по личному составу.

2.10.16. Документы, содержащие информацию по повышению квалификации и переподготовке сотрудника, его аттестация, служебное расследование.

2.10.17. Сведения о награждении государственными наградами Российской Федерации, присвоении почетных, воинских и специальных званий.

## 3. Обработка персональных данных

3.1. Общие требования при обработке персональных данных.

В целях обеспечения прав и свобод человека и гражданина при обработке персональных данных обязаны соблюдаться следующие требования:

3.1.1. Обработка персональных данных может осуществляться 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, контроля количества и качества выполняемой работы, обеспечения личной безопасности субъекта персональных данных и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества оператора.

3.1.2. Персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

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

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

3.1.5. Субъекты персональных данных, не являющиеся работниками, или их законные представители имеют право ознакомиться с документами оператора, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

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

3.2. Получение персональных данных.

3.2.1. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставление своих персональных данных и дает письменное согласие на их обработку оператором. Форма заявления-согласия субъекта на обработку персональных данных представлена в приложении 1 к настоящему Положению.

3.2.2. Письменное согласие не требуется, если обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных.

3.2.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. Форма отзыва согласия на обработку персональных данных представлена в приложении 2 к настоящему Положению.

3.2.4. В случаях, когда оператор может получить необходимые персональные данные субъекта только у третьей стороны, субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. В уведомлении оператор обязан сообщить о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа субъекта дать письменное согласие на их получение. Согласие оформляется в письменной форме в двух экземплярах: один из которых предоставляется субъекту, второй хранится у оператора. Форма заявления-согласия субъекта на получение его персональных данных от третьей стороны представлена в приложении 3 к настоящему Положению.

3.2.5. Запрещается получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни.

3.2.6. Запрещается получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.2.7. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации оператор вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

3.3. Хранение персональных данных.

3.3.1. Хранение персональных данных субъектов осуществляется отделом кадров и бухгалтерией на бумажных и электронных носителях с ограниченным доступом.

3.3.2. Личные дела хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела хранятся в специально отведенной секции сейфа, обеспечивающего защиту от несанкционированного доступа.

3.3.3. Подразделения, хранящие персональные данные на бумажных носителях, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденному постановлением Правительства РФ 15 сентября 2008 № 687.

3.4. Передача персональных данных

3.4.1. При передаче персональных данных субъекта оператор обязан соблюдать следующие требования:

– не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта или его законного представителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации или иными федеральными законами;

– предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило

соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;

– не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

– не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции;

– передавать персональные данные субъекта представителям субъектов в порядке, установленном Трудовым Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;

– все сведения о передаче персональных данных субъекта регистрируются в Журнале учета передачи персональных данных в целях контроля правомерности использования данной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана. Форма журнала учета передачи персональных данных представлена *в приложении 4* к настоящему Положению.

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

3.4.3. Внутренний доступ (доступ внутри организации) к персональным данным субъекта. Право доступа к персональным данным субъекта имеют:

– главный врач Учреждения;

– бухгалтер;

– сотрудник отдела кадров;

– непосредственные руководители по направлению деятельности (доступ к персональным данным сотрудников, непосредственно находящихся в его подчинении);

– сам субъект, носитель данных.

3.4.4. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных.

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

3.4.6. Организации, в которые субъект может осуществлять перечисления денежных средств (страховые Общества, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения) могут получить доступ к персональным данным субъекта только в случае его письменного разрешения.

3.5. Уничтожение персональных данных

3.5.1. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.5.2. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

## 4. Права и обязанности субъектов персональных данных и оператора

4.1. В целях обеспечения защиты персональных данных субъекты имеют право:

– получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

– требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;

– при отказе оператора или уполномоченного им лица исключить или исправить персональные данные субъекта - заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

– дополнить персональные данные оценочного характера заявлением, выражающим его собственную точку зрения;

– требовать от оператора или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать в суд любые неправомерные действия или бездействие оператора или уполномоченного им лица при обработке и защите персональных данных субъекта.

4.2. Для защиты персональных данных субъектов оператор обязан:

– за свой счет обеспечить защиту персональных данных субъекта от неправомерного их использования или утраты в порядке, установленном законодательством РФ;

– ознакомить работника или его представителей с настоящим Положением и его правами в области защиты персональных данных под расписку;

– по запросу ознакомить субъекта персональных данных, не являющегося работником, или в случае недееспособности либо несовершеннолетия субъекта, его законных представителей с настоящим Положением и его правами в области защиты персональных данных;

– осуществлять передачу персональных данных субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;

– предоставлять персональные данные субъекта только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей в соответствии с настоящим Положением и законодательством Российской Федерации;

– обеспечить субъекту свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством;

– по требованию субъекта или его законного представителя предоставить ему полную информацию о его персональных данных и обработке этих данных, форма журнала учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных представлена в приложении 5 к настоящему Положению.

4.3. Субъект персональных данных или его законный представитель обязуется предоставлять персональные данные, соответствующие действительности.

## 5. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

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

5.2. 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.

Заместитель главного врача по
правовым и кадровым вопросам Н.М. Мамавко

Приложение 1
к Положению об обработке
и защите персональных данных

Согласие на обработку персональных данных
медицинского работника

Я,_____
(фамилия, имя, отчество полностью)
Паспорт серия _____№_____ кем и когда выдан
___ _____ «_____»_____201_г.
Зарегистрирован по адресу: _____
_____

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ (ред. от 25.07.2011) «О персональных данных», своей волей и в своем интересе выражаю _____,
(Наименование медицинской организации)
зарегистрированному по адресу: _____
_____,
(Юридический адрес учреждения)
согласие на обработку моих персональных данных, включая выполнение действий по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, обезличиванию, блокированию, удалению, передаче Красноярскому краевому медицинскому информационно-аналитическому центру (ККМИАЦ) для внесения в федеральный регистр медицинских работников, а также Территориальному фонду обязательного медицинского страхования Красноярского края, органам государственной власти в целях обеспечения контроля и мониторинга финансового обеспечения оплаты труда медицинских работников.

Состав обрабатываемых персональных данных:
Фамилия, имя, отчество, дата и место рождения, пол, гражданство, паспортные данные, семейное положение, место жительства, номер телефона, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), сведения: об образовании, о сертификате специалиста, о занимаемой должности, об оплате труда, о воинском учете, о трудовой деятельности и другие сведения, содержащиеся в федеральном регистре медицинских работников.

Настоящее согласие вступает в силу с момента его подписания и действует в течение сроков, установленных законодательством Российской Федерации.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«_____»_____201_ года _____
подпись, расшифровка подписи

Приложение 2
к Положению об обработке
и защите персональных данных

# Заявление об отзыве
# согласия на обработку персональных данных
# медицинского работника

Я,_____
(фамилия, имя, отчество полностью)
Паспорт серия _____№_____ кем и когда выдан
_____ «_____»_____201_г.
Зарегистрирован по адресу: _____
_____

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», настоящим заявлением отзываю данное мною согласие на обработку моих персональных данных, включая выполнение действий по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, обезличиванию, блокированию, удалению, передаче Красноярскому краевому медицинскому информационно-аналитическому центру (ККМИАЦ) для внесения в федеральный регистр медицинских работников, а также Территориальному фонду обязательного медицинского страхования Красноярского края, органам государственной власти в целях обеспечения контроля и мониторинга финансового обеспечения оплаты труда медицинских работников.

Настоящее заявление вступает в силу с момента его подписания и действует в течение сроков, установленных законодательством Российской Федерации.

«_____»_____201__ года _____
подпись, расшифровка подписи

Приложение 3
к Положению об обработке
и защите персональных данных

# Согласие на получение персональных данных медицинского работника от третьих лиц

Я,_____
(фамилия, имя, отчество полностью)
Паспорт серия _____№_____ кем и когда выдан
___ _____ «_____»_____201_г.
зарегистрирован по адресу: _____
_____

В соответствии с Федеральным законом от 27.07.2006 № 152 - ФЗ «О персональных данных», даю согласие

_____,
(Наименование медицинской организации)
зарегистрированному по адресу: _____
_____,
(Юридический адрес учреждения)
согласие на получение моих персональных данных о предыдущих местах работы и периодах трудовой деятельности от третьих лиц.

Настоящее согласие вступает в силу с момента его подписания и действует в течение сроков, установленных законодательством Российской Федерации.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«_____»_____201__ года _____
подпись, расшифровка подписи

Приложение 4
к Положению об обработке
и защите персональных данных

# Журнал учета передачи персональных данных

| № | Сведения о запрашивающем лице | Состав запрашиваемых персональных данных | Цель получения персональных данных | Отметка о передаче или отказе в передаче персональных данных | Дата передачи/отказа в передаче персональных данных | Подпись запрашивающего лица | Подпись ответственного сотрудника |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Приложение 5
к Положению об обработке
и защите персональных данных

# Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных

| № | Сведения о запрашивающем лице | Краткое содержание обращения | Цель получения информации | Отметка о предоставлении или отказе в предоставлении информации | Дата передачи/отказа в предоставлении информации | Подпись запрашивающего лица | Подпись ответственного сотрудника |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Приложение 3
к приказу главного врача
от 03.04.15 № 171

УТВЕРЖДАЮ:
Главный врач
КГБУЗ «КМКБ № 4»
_____ А. П. ФОКИНА
«03» 04 2015г.

ПОЛОЖЕНИЕ о защите информации
в информационной системе персональных данных
в краевом государственном бюджетном учреждении здравоохранения
«Красноярская межрайонная клиническая больница»

## 1. Общие положения

1.1.Настоящее «Положение о защите персональных данных в информационной системе персональных данных в КМКБ «КГБУЗ № 4» (далее – Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Приказом ФСТЭК России от 18.02.2013 № 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. Положение разработано в целях обеспечения безопасности персональных данных (далее – ПДн) при их обработке в информационной системе персональных данных «Республиканская медицинская информационная система» (далее – ИСПДн).

1.3. Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений при их обработке, порядок обучения персонала практике работы в ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

## 2. Порядок предоставления допуска пользователей к работе в ИСПДн

Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Первоначальный допуск пользователей к работе в ИСПДн осуществляется на основании приказа, который издается руководителем медицинского учреждения (далее Руководитель). В приказе определяется список сотрудников, допущенных к работе в ИСПДн.

2.2. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации и выполнения

необходимых мероприятий по обеспечению безопасности в ИСПДн руководителем назначается администратор безопасности.

2.3. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться, и работать в ИСПДн.

2.4. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя запрещено.

2.5. В дальнейшем, процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой (Приложение 1).

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

2.6. Заявку рассматривает и визирует руководитель, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем заявка передается администратору безопасности для внесения необходимых изменений в списки пользователей ИСПДн.

2.7. На основании заявки администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля, а также регистрацию персонального идентификатора и другие необходимые действия, указанные в заявке.

2.8. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты соответствующие требованиям безопасности указанной ИСПДн.

2.9. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное значение пароля, которое он обязан сменить при первом же входе в систему.

2.10. Исполненная заявка хранится у администратора безопасности.

Она может впоследствии использоваться:

- для восстановления полномочий пользователей после возникновения внештатных ситуаций;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

## 3. Порядок работы пользователей ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

3.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

3.2. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

3.3. Перед началом работы в ИСПДн, сотрудники учреждения, допущенные к работе с ПДн, принимают под роспись обязательство о неразглашении персональных данных (Приложение 2).

3.4. Вход пользователя в систему должен осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю.

3.5. Запись информации, содержащей ПДн, должна осуществляться только на машинные носители информации, соответствующим образом учтенные в Журнале учета защищаемых носителей информации (Приложение 3). Ответственным за ведение Журнала учета является администратор безопасности.

3.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

3.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и **обязан**:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

– хранить в тайне свой пароль (пароли). В соответствии с п. 7.5. данного Положения и с установленной периодичностью менять свой пароль (пароли);

– хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних месте;

– выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить администратора информационной безопасности в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

– фактов совершения попыток несанкционированного доступа (далее - НСД) к ИСПДн;

– несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн;

– отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

– некорректного функционирования установленных на компьютеры технических средств защиты;

– непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить ПДн на неучтенных машинных носителях информации;

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие ПДн;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению конфиденциальности ПДн;

- размещать средства отображения информации (монитор, принтер и т.п.) таким образом, чтобы с них существовала возможность визуального считывания информации посторонними лицами.

3.8. Администратор безопасности обязан:

– знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС) установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

– контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

– производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

– реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

– вводить описания пользователей ИСПДн в информационную базу системы разграничения доступа в ИСПДн;

– своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

– проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

– контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

– обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

– осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

– настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

– организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации;

– периодически тестировать функции СЗИ от НСД с использованием специальных средств анализа защищенности, особенно при изменении программной среды и полномочий исполнителей;

– восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

– вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

– периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядок и правила проведения антивирусного тестирования;

– проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

– обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание персональных данных на носителях информации);

– присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

– вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

## 4. Порядок резервирования и восстановления работоспособности технических средств, программного обеспечения, баз данных, защищаемой информации и средств защиты информации

4.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

4.2. К использованию, для создания резервной копии в ИСПДн, допускаются только зарегистрированные в Журнале учета носители.

4.3. Администратор безопасности обязан осуществлять периодическое резервное копирование персональных данных.

4.4. Носители информации, предназначенные для создания резервной копии и хранения персональных данных, выдаются установленным порядком администратором безопасности. По окончании процедуры резервного копирования электронные носители сдаются на хранение администратору безопасности, или руководителю.

4.5. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

4.6. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

4.7. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания, с целью предотвращения повреждения технических средств и(или) защищаемой информации в результате сбоев в сети электропитания.

4.8. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных.

4.9. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся у администратора безопасности. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

4.10. Ответственность за проведение резервного копирования, мероприятий по восстановлению работоспособности технических средств, мероприятий по восстановлению средств защиты информации возлагается на администратора безопасности.

## 5. Правила антивирусной защиты

Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение.

5.1. К использованию на компьютерах допускаются только лицензионные антивирусные средства;

5.2. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности;

5.3. Администратор безопасности осуществляет периодическое обновление антивирусных средств и контроль их работоспособности;

5.4. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы;

5.5. Еженедельно в начале работы, после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров;

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель);

5.6. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль;

5.7. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности

должна быть выполнена антивирусная проверка ИСПДн;

5.8. На компьютеры пользователей запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации;

5.9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить обработку данных в ИСПДн;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;

– совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов.

5.10. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности;

5.11. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

## 6. Правила парольной защиты

6.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

6.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

6.3. При доступе пользователя в систему должна осуществляться идентификация и проверка подлинности по идентификатору и паролю, а также с использованием электронных идентификаторов.

6.4. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями самостоятельно с учетом следующих требований:

- пароль должен быть длиной не менее шести буквенно-цифровых символов;
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

6.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

6.6. Удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри учреждения и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой, на основании указания руководителя или начальника отдела кадров.

6.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) администратора безопасности.

6.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по изменению его пароля.

6.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

## 7. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

7.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

7.2. Право на установку, обновление и модификацию общесистемного и прикладного программного обеспечения компьютеров ИСПДн предоставляется администратору безопасности.

7.3. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме администратора безопасности запрещено.

7.4. Заявку на внесение изменений в конфигурацию аппаратно-программных средств защищенных рабочих мест ИСПДн, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке.

7.5. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

7.6. Установка и обновление ПО (системного, прикладного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.).

7.7. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

7.8. После установки (обновления) ПО, администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки.

7.9. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, администратор безопасности обязан предпринять

необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

## 8. Порядок контроля обеспечения защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления.

8.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

8.2. Основными задачами контроля являются:

– проверка организации выполнения мероприятий по защите информации в учреждении, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;

– выявление демаскирующих признаков объектов ИСПДн;

– уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

– проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

– проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

– проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

– проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

– оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;

– разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

## 9. Перечень персональных данных подлежащих защите

9.1.Требования, предъявляемые к основным мероприятиям по технической защите персональных данных, которые должны быть реализованы в рамках системы защиты персональных данных в многопользовательских информационных систем 3-го класса (К3) с разными правами доступа пользователей к защищаемым информационным активам. Итак, согласно действующим требованиям в информационной системе данного класса должны быть реализованы:

- идентификация и аутентификация пользователей по паролю длиной не менее 6 символов;

• управление доступом к защищаемой информации;

• регистрация в журналах аудита "входа"/"выхода" в систему/из системы;

• учет носителей, содержащих конфиденциальную информацию (персональные данные) с регистрацией их выдачи/приема;

• целостность программных средств защиты информации от несанкционированного доступа;

• неизменность программной среды информационной системы;

• физическая охрана физических активов информационной системы, включая носителей конфиденциальной информации;

• периодическое тестирование системы защиты персональных данных;

• механизмы восстановления системы защиты персональных данных;

• межсетевое экранирование - вне зависимости от наличия подключения к сети Интернет;

• антивирусная защита информационной системы.

9.2. Информационные системы, применяемые в КГБУЗ «КМКБ № 4» и использующие персональные данные, делятся на 2 группы.

1. ИС, использующие персональные данные сотрудников.
2. ИС, использующие персональные данные пациентов

К первой группе относятся:

1. Программа ПЭО «Парус-7» (К3)
2. Регистр медицинских работников(РМР) (К3)
3. Программа пенсионного фонда(Документы ПУ5 ) (К3)

Ко второй группе относятся:

1. РМИС qMS
2. Стационар
3. Поликлиника
4. Видар

9.3. ИС первой группы относятся к классу К3 используют следующие персональные данные:

• Фамилия, имя, отчество сотрудника

• Место, год и дата рождения

• Адрес по прописке

• Паспортные данные (серия, номер паспорта, кем и когда выдан)

• Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность)

• Информация о трудовой деятельности до приема на работу

• Информация о трудовом стаже (место работы, должность, период работы, период работы, причины увольнения)

• Адрес проживания (фактический)

• Телефонный номер (домашний, рабочий, мобильный)

• Семейное положение и состав семьи

• Информация о знании иностранных языков

• Форма допуска

• Оклад

• Данные о трудовом договоре

• Сведения о воинском учете

- ИНН
- Данные об аттестации работников
- Данные о повышении квалификации
- Данные о наградах, медалях, поощрениях, почетных званиях
- Информация о приеме на работу, перемещении по должности, увольнении
- Информация об отпусках
- Информация о командировках
- Информация о негосударственном пенсионном обеспечении

9.4. Согласно действующим требованиям в информационной системе данного класса должны быть реализованы:

- идентификация и аутентификация пользователей по паролю длиной не менее 6 символов;
- управление доступом к защищаемой информации;
- регистрация в журналах аудита "входа"/"выхода" в систему/из системы;
- учет носителей, содержащих конфиденциальную информацию (персональные данные) с регистрацией их выдачи/приема;
- целостность программных средств защиты информации от несанкционированного доступа;
- неизменность программной среды информационной системы;
- физическая охрана физических активов информационной системы, включая носителей конфиденциальной информации;
- периодическое тестирование системы защиты персональных данных;
- механизмы восстановления системы защиты персональных данных;
- межсетевое экранирование - вне зависимости от наличия подключения к сети Интернет;
- антивирусная защита информационной системы.

9.5. Персональные данные, используемые ИС второй группы, относящейся к классу К1:

- Фамилия, имя, отчество пациента
- Место, год и дата рождения
- Адрес по прописке
- Паспортные данные (серия, номер паспорта, кем и когда выдан)
- Адрес проживания (фактический)
- Телефонный номер (домашний, рабочий, мобильный)
- Семейное положение и состав семьи
- Информация о болезнях
- Диагнозы, описание заболеваний, методы их лечения.

**9.6. Программа ПЭО «Парус-7»**

Некоторые модули этого программного комплекса используют персональные данные. В частности, модуль «Заработная плата» и «Кадры». Это многопользовательские модули, база данных которых располагается на сервере организации.

Защита персональных данных, используемых в этих модулях, осуществляется с помощью разграничения прав доступа введением логинов и паролей пользователей.

Пользователями этой программы являются специалисты подразделений:

- бухгалтерия
- экономический отдел

• отдел кадров

• отдел АСУ

Администратором ИСПДн и администратором безопасности этой ИС является программист Минчаков Сергей Викторович.

**9.7. Регистр медицинских работников(РМР)**

Программа используется как однопользовательская в отделе кадров. Содержит персональную информацию о всех работниках учреждения. Администратором ИСПДн и администратором безопасности этой ИС является ведущий инженер-программист отдела АСУ Булахов Игорь Валерьевич.

**9.8. Программа пенсионного фонда (Документы ПУ5 )**

Программа используется как многопользовательская. Содержит персональную информацию о всех работниках учреждения.

Пользователями этой программы являются специалисты подразделений :

• бухгалтерия

• отдел кадров

Администратором ИСПДн и администратором безопасности этой ИС является ведущий инженер-программист отдела АСУ Булахов Игорь Валерьевич.

**9.9.РМИС qMS**

Программа используется как многопользовательская. Содержит персональную информацию о пациентах и работниках учреждения. Доступ к базе данных осуществляется с помощью интернет.

Пользователями этой программы являются специалисты подразделений :

• бухгалтерия

• отдел кадров

• экономисты

• стационар со всеми подразделениями

• КДО

• отдел статистики

• отдел АСУ

Администратором ИСПДн и администратором безопасности этой ИС является начальник отдела АСУ Азеев Егор Александрович.

**9.10. Программа «Стационар»**

Программа используется как многопользовательская. Содержит персональную информацию о пациентах учреждения.

Пользователями этой программы являются специалисты подразделений :

• отдел статистики

• подразделения параклиники

• отдел АСУ

Администратором ИСПДн и администратором безопасности этой ИС является ведущий инженер-программист отдела АСУ Стальнова Антонина Валентиновна.

**9.11. Программа «Поликлиника»**

Программа используется как многопользовательская. Содержит персональную информацию о пациентах лечебно-диагностического отделения учреждения.

Пользователями этой программы являются специалисты подразделений :

• отдел статистики лечебно-диагностического отделения

• регистратура лечебно-диагностического отделения

• отдел АСУ

Администратором ИСПДн и администратором безопасности этой ИС является ведущий инженер-программист отдела АСУ Стальнова Антонина Валентиновна.

**9.12. Программа «Видар»**

Программа используется как многопользовательская. Содержит персональную информацию о пациентах отделения УЗД учреждения.

Пользователями этой программы являются специалисты подразделений:

- отделения УЗД
- отдел АСУ

Администратором ИСПДн и администратором безопасности этой ИС является начальник отдела АСУ Азеев Егор Александрович.

## 10.Порядок охраны и допуска посторонних лиц в помещения ИСПДн

10.1. В помещениях должна быть установлена охранная и пожарная сигнализация.

10.2. Серверное и коммутационное оборудование ИСПДн должно находиться под надежным замком, в отдельном помещении или запирающемся шкафу, ключ должен храниться у администратора безопасности.

10.3. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения утверждается руководителем и передаётся на пост охраны.

10.4. При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, убираются для хранения в запираемый ящик стола или сейф.

10.5. При обнаружении повреждения замков, дверей или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт, в присутствии охранника. О происшествии немедленно сообщается руководителю и(или) ответственному за защиту информации.

10.6. При срабатывании охранной сигнализации в служебных помещениях в нерабочее время охранник сообщает о случившемся ответственному за помещение, или ответственному за защиту информации, или руководителю, или администратору безопасности.

## 11.Заключительные положения

11.1. Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих персональные данные.

11.2. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Заместитель главного врача по
правовым и кадровым вопросам — Н.М. Мамавко

Приложение 1
к Положению о защите информации

# ЗАЯВКА

на внесение изменений в списки пользователей и наделение их полномочиями доступа к ресурсам информационной системы персональных данных КГБУЗ «КМКБ № 4»

Прошу зарегистрировать пользователем (исключить из списка пользователей, изменить полномочия пользователя) информационной системы персональных данных КГБУЗ «Красноярская межрайонная клиническая больница № 4»

_____ ,

(должность с указанием подразделения)

_____

(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых) для решения задач:

_____

(список задач, приложений)

на следующих рабочих местах

_____

_____ _____

(фамилия, инициалы) (подпись)

«_____» _____ _____г.

Приложение 2
к Положению о защите информации

# ОБЯЗАТЕЛЬСТВО
## о неразглашении информации, содержащей персональные данные

Я, _____,
(Ф.И.О. сотрудника)

_____,
(должность)

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. В течение года после прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден (а) о том, что в случае нарушения данного обязательства буду привлечен (а) к дисциплинарной ответственности и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____ _____
(фамилия, инициалы) (подпись)

«____» _____ _____г.

Приложение 3
к Положению о защите информации

# ЖУРНАЛ УЧЕТА
## защищаемых носителей информации

Начат __.__.201___ г.

Администратор информационной безопасности
ФИО

| Дата поступления | Учетный номер | Вид носителя | Заводской (серийный номер) | Расписка в получении (ФИО, подпись, дата) | Расписка в обратном приеме (ФИО, подпись, дата) | Место хранения | Отметка об уничтожении бракованных МНИ (№ акта, подпись, дата) |
|---|---|---|---|---|---|---|---|
| 25.05.2010 | 1-пдн | НЖДМ | ST09545001AS | | | | |
| 25.05.2010 | 2-пдн | ЭП | | | | | |
| 25.05.2010 | 3-пдн | ЭП | | | | | |
| | | | | | | | |

НЖМД - накопитель на жестких магнитных дисках;
ГД - гибкие магнитные диски;
ОД - оптические и магнитооптические диски;
ЭП - устройства долговременной электронной памяти (Flash Memory);
МЛ - магнитные ленты.

Приложение 4
к Положению о защите информации

# ЖУРНАЛ УЧЕТА
сертифицированных средств защиты информации,
эксплуатационной и технической документации к ним

Начат __.__.201__ г.

Администратор информационной безопасности
ФИО

| Номер п/п | Индекс и наименование средства защиты информации | Серийный (заводской) номер | Номер специального защитного знака | Наименование организации, установившей СЗИ | Место установки | Примечание |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |