

«Утверждаю»
Главный врач
ГБУЗ «ГДБ г. Коркино»

 А.И. Земянский

(Приложение 2
к приказу № 25од от 30.12.2022)

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ
«ГОРОДСКАЯ ДЕТСКАЯ БОЛЬНИЦА Г.КОРКИНО»

г. Коркино
2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных (далее — Положение) государственного бюджетного учреждения здравоохранения «Городская детская больница г. Коркино» (далее Учреждения) разработано в соответствии с Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ, Гражданским кодексом Российской Федерации от 30.11.1994 № 51-ФЗ, Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации.

1.2. Цели разработки Положения:

1.2.1. определение порядка обработки персональных данных сотрудников и пациентов, а также иных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий Учреждения;

1.2.2. обеспечение защиты прав и свобод человека и гражданина, в т.ч. сотрудников и пациентов Учреждения, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

1.2.3. установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. К любой информации, содержащей персональные данные субъекта, применяется режим конфиденциальности, за исключением:

1.3.1. обезличенных персональных данных;

1.3.2. общедоступных персональных данных.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом Российской Федерации.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.2. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.3. **Документированная информация** - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. **Информация** - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.5. **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

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

блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.7. Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека (Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утв. постановлением Правительства РФ от 15.09.2008 № 687)

2.8. Оператор - Учреждение.

2.9. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.10. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.11. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

3. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Состав персональных данных, обрабатываемых в Учреждении, определяется «Перечнем сведений, содержащих персональные данные» (Приложение 1).

3.2. Документы со сведениями, содержащими персональные данные, обрабатываются в следующих структурных подразделениях учреждения:

- 3.2.1. поликлиника
- 3.2.2. отдел кадров
- 3.2.3. экономический отдел
- 3.2.4. информационно-аналитический отдел
- 3.2.5. отдел информатизации и информационной безопасности;
- 3.2.6. дневной стационар при поликлинике
- 3.2.7. стационар на дому

4. ПОРЯДОК ПОЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.

4.2. Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме, в соответствии с утвержденной в Учреждении формой такого Согласия.

4.3. Комплекс документов, сопровождающий процесс взаимодействия с соискателями вакантной должности:

4.3.1. При наличии вакансии, поиск кандидатов на вакантную должность осуществляется через центр занятости населения, так же выкладывается информация о вакансии на сайт Учреждения. По результатам собеседования кандидата с главным врачом принимается решение о трудоустройстве кандидата на вакантную должность.

4.3.2. В случае если сотрудник отдела кадров Учреждения получил резюме в электронном виде, но в данный момент не существует вакантной должности для данного соискателя, сотрудник отдела кадров уничтожает резюме в течении 5 (Пяти) дней.

4.4. Комплекс документов, сопровождающий процесс оформления трудовых отношений сотрудника Учреждения при его приёме, переводе и увольнении:

4.4.1. Информация, представляемая сотрудником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в

соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

4.4.1.1. паспорт или иной документ, удостоверяющий личность;

4.4.1.2. трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;

4.4.1.3. страховое свидетельство государственного пенсионного страхования;

4.4.1.4. документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;

4.4.1.5. документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

4.4.1.6. свидетельство о присвоении ИНН (при его наличии у сотрудника).

4.4.2. При оформлении сотрудника в Учреждение сотрудником отдела кадров заполняется унифицированная форма Т-2 «Личная карточка сотрудника».

4.4.3. Вся необходимая информация копируется в ИСПДн «Персонал».

4.4.4. В отделе кадров Учреждения создаются и хранятся следующие группы документов, содержащие персональные данные сотрудников в единичном или сводном виде:

4.4.4.1. документы, содержащие персональные данные сотрудников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки сотрудников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации сотрудников; материалы служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений; копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения);

4.4.4.2. документация по Учреждению, работе отделов (положения, должностные инструкции сотрудников, приказы главного врача);

4.4.4.3. документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

4.5. Комплекс документов, сопровождающий процесс работы с пациентами.

4.5.1. Информация, представляемая пациентами, либо их представителями в структурные подразделения Учреждения, должна иметь документальную форму. Пациенты, либо их представители предъявляют следующие документы:

4.5.1.1. паспорт или иной документ, удостоверяющий личность;

4.5.1.2. страховой полис обязательного медицинского страхования;

4.5.1.3. страховое свидетельство государственного пенсионного страхования.

4.5.2. Данные из документов вносятся сотрудниками в электронном виде в ИСПДн «Пациенты». В бумажном виде впоследствии создаются, хранятся и передаются следующие группы документов, содержащие персональные данные пациентов Учреждения в единичном или сводном виде:

4.5.2.1. талон амбулаторного пациента форма 025-12/у;

4.5.2.2. медицинская карта амбулаторного пациента форма № 025/у-04;

4.5.2.3. медицинская карта стационарного больного форма № 003/у;

4.5.2.4. статистическая карта выбывшего из стационара формы №066/у-02;

4.5.2.5. другая утвержденная Минздравсоцразвития РФ документация и справки по месту требования, в соответствии с законом.

5. ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Хранение бумажных документов, электронных носителей (дискет, дисков и т.п.), содержащих персональные данные, должно осуществляться в специальных папках, закрытых шкафах или сейфах, в порядке, исключающем доступ к ним третьих лиц.

5.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации, удовлетворяющие устанавливаемым в соответствии с законодательством РФ требованиям, обеспечивающим защиту информации.

5.3. Обработка персональных данных в Учреждении осуществляется до утраты правовых оснований обработки персональных данных. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в Учреждении определяются «Перечнем сведений, содержащих персональные данные» (Приложение 1).

5.4. По истечении срока хранения документы, либо иные материальные носители персональных данных должны быть уничтожены без возможности восстановления (например, в бумагорезательных машинах) с составлением акта. Для машинных носителей допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ (например, «Safe Erase», «Eraser», «FDelete») без уничтожения материального носителя.

5.5. Обезличивания персональных данных в Учреждении в настоящее время не предполагается.

6. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных может осуществляться исключительно 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), осуществления трудовых (договорных) отношений, и в случаях, установленных законодательством Российской Федерации.

6.2. При определении объема и содержания, обрабатываемых персональных данных Учреждение руководствуется Конституцией Российской Федерации от 25.12.1993, Трудовым кодексом Российской Федерации от 30.12.2001 №197-ФЗ, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Федеральным законом от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и иными нормативно-правовыми актами Российской Федерации, а также настоящим Положением.

7. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Передавать персональные данные субъектов допускается только тем сотрудникам, которые имеют допуск к обработке персональных данных.

7.2. Предоставление персональных данных допускается в случаях передачи Федеральной налоговой службе, Социальному фонду России, банковским учреждениям РФ с целью зачисления заработной платы на личный счет сотрудника, Фонду обязательного медицинского страхования, другим медицинским учреждениям, Министерству здравоохранения Челябинской области, Челябинскому областному медицинскому информационно-аналитическому центру, раскрытия данных правоохранительным органам при наличии законных оснований, а также в иных случаях, установленных законодательством РФ.

7.3. Не допускается распространение персональных данных субъекта.

8. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. Защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением за счет бюджетных и своих средств.

8.2. В Учреждении защите подлежат все сведения, содержание персональные данные субъектов, в том числе:

- 8.2.1. зафиксированные в бумажных документах;
 - 8.2.2. зафиксированные в электронных документах на технических средствах, включая внешние носители;
 - 8.2.3. речевая (акустическая) информация, содержащая персональные данные;
 - 8.2.4. текстовая и графическая видовая информация, содержания персональные данные;
- 8.3. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:
- 8.3.1. Проведение организационных мероприятий:
 - 8.3.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;
 - 8.3.1.2. ознакомление сотрудников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;
 - 8.3.1.3. организация учёта носителей персональных данных;
 - 8.3.1.4. разработка модели угроз безопасности персональным данным;
 - 8.3.1.5. проведение обучения сотрудников вопросам защиты персональных данных.
 - 8.3.2. Программно-аппаратная защита:
 - 8.3.2.1. внедрение программно-аппаратных средств защиты информации, прошедших в соответствии с Федеральным законом №184 от 27.12.2002 г. «О техническом регулировании» оценку соответствия;
 - 8.3.3. Инженерно-техническая защита:
 - 8.3.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;
 - 8.3.3.2. установка усиленных дверей, сигнализации, режима охраны здания и помещений, в которых обрабатываются персональные данные.
- 8.4. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами Учреждения.
- 8.5. Организацию и контроль защиты персональных данных в структурных подразделениях Учреждения осуществляют их непосредственные руководители.

9. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

- 9.1. Допуск к персональным данным субъекта могут иметь только те сотрудники Учреждения, которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей.
- 9.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:
- 9.2.1. ознакомление сотрудника с настоящим Положением, «Инструкцией о порядке работы с персональными данными» и другими локальными нормативно-правовыми актами Учреждения, касающимися обработки персональных данных;
 - 9.2.2. истребование с сотрудника «Обязательства о неразглашении персональных данных пациентов» и (или) «Обязательства о неразглашении персональных данных работников»;
- 9.3. Каждый сотрудник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.
- 9.4. Сотрудникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.
- 9.5. Специалисты Учреждения, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее – пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за организацию обработки персональных данных.

10. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

10.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

10.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

10.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники Учреждения или лица, осуществляющие такую обработку по договору с Учреждением), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти Челябинской области, а также локальными правовыми актами Учреждения.

10.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

10.4.1. типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Учреждением способов обработки персональных данных;

10.4.2. типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку персональных данных;

10.4.3. типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

10.5. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение Учреждения или в иных аналогичных целях, должны соблюдаться следующие условия:

10.5.1. необходимость ведения такого журнала должна быть предусмотрена актом Учреждения, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

10.5.2. копирование содержащейся в таких журналах информации не допускается;

10.5.3. персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более 1 (Одного) раза в каждом случае пропуска субъекта персональных данных.

10.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки

иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

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

11. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Состав информационных систем персональных данных Учреждения и их характеристика определяется «Перечнем информационных систем персональных данных» (Приложение 2).

11.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

11.3. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

11.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством РФ порядке.

11.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

11.6. Размещение информационных систем, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

11.7. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за организацию обработки персональных данных в ИСПДн.

11.8. При обработке персональных данных в информационной системе должно быть обеспечено:

11.8.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

11.8.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

11.8.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

11.8.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

11.8.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

11.9. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

11.9.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

11.9.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

11.9.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

11.9.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

11.9.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

11.9.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

11.9.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

11.9.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

11.9.9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

11.9.10. описание системы защиты персональных данных.

11.10. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе возлагается на инженера-программиста.

11.11. Список лиц, имеющих доступ к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается приказом главного врача.

11.12. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

11.12.1. Иные требования по обеспечению безопасности информации и средств защиты информации в Учреждении выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти Челябинской области.

12. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

12.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

12.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

12.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом главного врача.

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

13.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, ответственного за обеспечение безопасности персональных данных ИСПДн и ответственного за организацию обработки персональных данных Учреждения.

13.2. Сотрудники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

13.2.1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) Учреждения, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник Учреждения, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Учреждению (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

13.2.2. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьями Кодекса об административных правонарушениях РФ.

13.2.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

13.3. Сотрудник Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно статей Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

14.1. Настоящее Положение утверждается главным врачом и является обязательным для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

14.2. Все сотрудники Учреждения, участвующие в обработке персональных данных, должны быть ознакомлены с настоящим Положением под подпись.

ПЕРЕЧЕНЬ

сведений, содержащих персональные данные

1. СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ:

- 1.1. Сведения, составляющие персональные данные сотрудников:
 - 1.1.1. фамилия, имя, отчество;
 - 1.1.2. ИНН;
 - 1.1.3. СНИЛС;
 - 1.1.4. табельный номер;
 - 1.1.5. пол;
 - 1.1.6. номер, дата трудового договора;
 - 1.1.7. дата рождения;
 - 1.1.8. место рождения
 - 1.1.9. гражданство;
 - 1.1.10. наименование и степень знания иностранного языка;
 - 1.1.11. образование (среднее (полное) общее, начальное профессиональное, среднее профессиональное, высшее профессиональное, аспирантура, адъюнктура, докторантура);
 - 1.1.12. наименование образовательного учреждения;
 - 1.1.13. наименование, серия, номер, дата выдачи, направление или специальность, код по ОКСО, ОКИН документа об образовании, о квалификации или наличии специальных знаний
 - 1.1.14. профессия (в т.ч. код по ОКПДТР);
 - 1.1.15. стаж работы;
 - 1.1.16. состояние в браке;
 - 1.1.17. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;
 - 1.1.18. данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ);
 - 1.1.19. адрес и дата регистрации;
 - 1.1.20. фактический адрес места жительства;
 - 1.1.21. контактная информация (телефон / e-mail);
 - 1.1.22. сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС; категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета);
 - 1.1.23. реквизиты военного билета (серия, номер, дата выдачи, орган выдавший документ)
 - 1.1.24. дата приема на работу;
 - 1.1.25. характер работы;
 - 1.1.26. вид работы (основной, по совместительству);
 - 1.1.27. структурное подразделение;
 - 1.1.28. занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации;
 - 1.1.29. ранее занимаемая должность;
 - 1.1.30. тарифная ставка (оклад), надбавка, руб.
 - 1.1.31. основание трудоустройства;
 - 1.1.32. личная подпись сотрудника; сведения об аттестации (дата, решение, номер и дата документа, основание);
 - 1.1.33. сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа свидетельствующего о переподготовке, основание переподготовки);
 - 1.1.34. сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды);

- 1.1.35. сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание);
- 1.1.36. сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание);
- 1.1.37. сведения об увольнении (основания, дата, номер и дата приказа);
- 1.1.38. объем работы;
- 1.1.39. сведения о доходах;
- 1.1.40. сведения из трудовой книжки, водительского удостоверения, медицинской справки о допуске к управлению автомобиля;
- 1.1.41. сведения о судимости (для сотрудников работающих с детьми);
- 1.1.42. сведения о состоянии здоровья сотрудника (медицинская книжка).
- 1.2. Сведения, составляющие персональные данные пациентов:
 - 1.2.1. фамилия, имя, отчество;
 - 1.2.2. пол;
 - 1.2.3. дата рождения;
 - 1.2.4. место рождения;
 - 1.2.5. семейное положение;
 - 1.2.6. состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения ближайших родственников;
 - 1.2.7. социальный статус;
 - 1.2.8. адрес и дата регистрации;
 - 1.2.9. фактический адрес жительства;
 - 1.2.10. контактная информация (телефон / e-mail);
 - 1.2.11. реквизиты свидетельства о рождении (серия, номер, дата выдачи, орган выдавший документ);
 - 1.2.12. реквизиты паспорта (серия, номер, дата выдачи, орган выдавший документ);
 - 1.2.13. реквизиты военного билета (серия, номер, дата выдачи, орган выдавший документ);
 - 1.2.14. данные полиса обязательного медицинского страхования или добровольного медицинского страхования;
 - 1.2.15. СНИЛС;
 - 1.2.16. данные об инвалидности;
 - 1.2.17. данные о льготах;
 - 1.2.18. данные о месте работы, подразделении, должности (профессии);
 - 1.2.19. данные о месте учебы, классе (группе);
 - 1.2.20. данные об антропометрии;
 - 1.2.21. данные о состоянии здоровья;
 - 1.2.22. данные о заболеваниях;
 - 1.2.23. данные лабораторных и параклинических исследований;
 - 1.2.24. данные о случаях обращения за медицинской помощью с любой целью;
 - 1.2.25. ИНН;
 - 1.2.26. номер карты амбулаторного больного;
 - 1.2.27. номер медицинской карты;
 - 1.2.28. дата и время посещения врача;
 - 1.2.29. состояние алкогольного/наркотического опьянения;
 - 1.2.30. дата поступления в приемное отделение;
 - 1.2.31. дата выписки;
 - 1.2.32. результат госпитализации.
 - 1.2.33. другие данные, относящиеся к персональным данным пациента, и дающие возможность идентифицировать его

2. ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- 2.1. Конституция Российской Федерации от 25.12.1993;
- 2.2. Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ;
- 2.3. Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ;
- 2.4. Налоговый Кодекс Российской Федерации часть первая от 31 июля 1998 г. N 146-ФЗ и часть вторая от 5 августа 2000 г. N 117-ФЗ;
- 2.5. Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- 2.6. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»;
- 2.7. Федеральный закон от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности»;
- 2.8. «Основы законодательства Российской Федерации об охране здоровья граждан» № 5487-1 от 22.07.1993 г.;
- 2.9. Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»;
- 2.10. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- 2.11. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- 2.12. Федеральный закон от 29.11.2010 №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- 2.13. Федеральный закон от 21.11.2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- 2.14. Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера»;
- 2.15. Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 2.16. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 2.17. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
- 2.18. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- 2.19. Приказ Минздравсоцразвития России от 12.04.2011 N 302н (ред. от 15.05.2013) «Об утверждении перечней вредных и (или) опасных производственных факторов и работ, при выполнении которых проводятся обязательные предварительные и периодические медицинские осмотры (обследования), и Порядка проведения обязательных предварительных и периодических медицинских осмотров (обследований) работников, занятых на тяжелых работах и на работах с вредными и (или) опасными условиями труда»;
- 2.20. Лицензия на осуществление медицинской деятельности № ЛО-74-01-005511 от 22 апреля 2020 года;
- 2.21. Устав государственного бюджетного учреждения здравоохранения «Городская детская больница г. Коркино».

ПЕРЕЧЕНЬ
Информационных систем персональных данных (ИСПДн)

№ п/п	Наименование ИСПДн	Наименование и адрес объекта
1	2	3
1	ИСПДн «Персонал»	Государственное бюджетное учреждение здравоохранения "Городская детская больница г.Коркино", Коркинский муниципальный район, г. Коркино, ул. 9 января, д. 38/1
2	ИСПДн «Пациенты»	Государственное бюджетное учреждение здравоохранения "Городская детская больница г.Коркино", Коркинский муниципальный район, г. Коркино, ул. 9 января, д. 38/1