Управление здравоохранения города Ростова-на-Дону
Муниципальное бюджетное учреждение здравоохранения
«Городская поликлиника № 12
города Ростова-на-Дону»

ПРИКАЗ

«27» 08 2018г. № 132

Об организации обработки, учета,
хранения и защиты персональных данных
в МБУЗ «Городская поликлиника №12 г.
Ростова-на-Дону»

В соответствии с Федеральным законом Российской Федерации от 26.07.2006 № 152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1.Утвердить положение об обработке и защите персональных данных работников и пациентов МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» в соответствии с приложением №1 к настоящему приказу.
2.Утвердить инструкцию по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» в соответствии с приложением №2 к настоящему приказу
3.Назначить администратором информационных систем персональных данных (ИСПДн) и ответственным за антивирусную защиту в МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» рабочего по комплексному обслуживанию и ремонту зданий Волгина Илью Валерьевича.
4.Утвердить инструкцию по порядку учета и хранению документов, содержащих персональные данные, в МБУЗ «городская поликлиника №12 г. Ростова-на-Дону» в соответствии с приложением №3 к настоящему приказу.
5.Утвердить инструкцию пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в муниципальном бюджетном учреждении здравоохранения «Городская поликлиника №12 г. Ростова-на-Дону» в соответствии с приложением №4 к настоящему приказу.
6.Утвердить порядок доступа сотрудников МБУЗ «Городская поликлиника №12 г Ростова-на-Дону» в помещения, в которых ведется обработка персональных данных в соответствии с приложением №5 к настоящему приказу.
7.Утвердить инструкцию по организации антивирусной защиты в информационных системах персональных данных МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» в соответствии с приложением №6 к настоящему приказу.
8.Утвердить список должностей, имеющих доступ к персональным данным в соответствии с приложением №7 к настоящему приказу.
14 Контроль исполнения настоящего приказа оставляю за собой.

Главный врач А.В. Божко

Приложение № 1

к приказу МБУЗ «Городская
поликлиника №12 г Ростова-на-Дону»

от 24.08.18 № 132

Положение
об обработке и защите персональных данных работников и пациентов
МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону»

I. Общие положения

1.1. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных субъектов (работников и пациентов), осуществляемое МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону», именуемое по тексту «учреждение здравоохранения», «оператор», а также порядок ведения их личных дел, медицинских карт.
1.2. Цель настоящего Положения - обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных сотрудников, пациентов, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных.
1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» (в ред. ФЗ от 25.07.2011 №261-ФЗ), Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.2004г. №98-ФЗ «О коммерческой тайне», Федеральным законом от 22.10.2004г. № 125-ФЗ «Об архивном деле в Российской Федерации». Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 №323-ФЗ
1.4. В настоящем Положении используются следующие термины и определения:
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 МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону».
Субъект персональных данных (субъект) - физическое лицо (работник или пациент), которое может быть однозначно идентифицировано по персональным данным.
Персональные данные (ПД) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации в области трудовых отношений и здравоохранения, Положением об обработке и защите персональных данных и приказами МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону».
Обработка персональных данных - действия (операции) с персональными данными, включая систематизацию, накопление, хранение, комбинирование, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
Защита персональных данных - деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и обеспечение организационно-технических мер защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения.
Конфиденциальная информация - это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.
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 информационнотелекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

II. Сбор и обработка персональных данных субъектов персональных данных

2.1. Сбор и обработка персональных данных осуществляется исключительно с письменного согласия субъекта. Образцы форм заявления о согласии на обработку персональных данных и отказа от нее, размещены в Приложении 1, Приложении 2 и Приложении 3, Приложение 4 к настоящему положению. Персональные данные субъекта ПД относятся к конфиденциальной информации. Требования при обработке персональных данных субъекта (работника) установлены ст. 86 Трудового кодекса РФ и не подлежат изменению и исключению.
2.2. В целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных субъекта ПД обязаны соблюдать следующие общие требования:
2.2.1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, количества и качества выполняемой работы, обследования, наблюдения и лечения пациентов и обеспечения сохранности имущества оператора, субъекта и третьих лиц.
2.2.2. Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания персональных данных.
2.2.3. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ, Федеральным законом «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 №323-ФЗ и иными федеральными законами.
2.2.4. Информация о персональных данных субъекта предоставляется оператору субъектом устно, либо путем заполнения личных карточек формы Т-2 для работников (медицинских карт, историй болезней - для пациентов), которые хранятся в личном деле в отделе кадров (регистратуре/архиве). Если персональные данные субъекта возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.
2.2.5. Оператор не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и частной жизни. 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.
2.2.6. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.
2.2.7. При принятии решений, затрагивающих интересы субъекта, оператор не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.
2.3. При поступлении на работу субъекта представляет сотрудникам отдела кадров следующие документы, содержащие персональные данные о себе:
- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается
впервые или работник поступает на работу на условиях совместительства;
- страховое свидетельство государственного пенсионного страхования;

- свидетельство о регистрации индивидуального налогового номера (ИНН);
- документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки.

2.4. При приеме к врачу пациент представляет следующие документы, содержащие персональные данные о себе:
- паспорт или иной документ, удостоверяющий личность, гражданство;
- полис ОМС;
- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);
- в отдельных случаях с учетом специфики обследования в учреждение здравоохранение действующим законодательством РФ может предусматриваться необходимость предъявление дополнительных документов.

2.5. Запрещается требовать от лица, поступающего на работу (или прием), документа помимо предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации.

2.6. При заключении трудового договора и в ходе трудовой деятельности может возникнуть необходимость в предоставлении субъектам документов:
- о возрасте детей;
- об инвалидности;
- о донорстве;
- о составе семьи;
- о необходимости ухода за больным членом семьи;
- прочие.

2.7. После того, как будет принято решение о приеме субъекта на работу, а также впоследствии в процессе трудовой деятельности, к документам, содержащим персональные данные субъекта, также будут относиться:
- трудовой договор;
- приказ о приеме на работу;
- приказы о поощрениях и взысканиях;
- результаты медицинского осмотра сотрудника при приеме на работу;
- приказы, связанные с прохождением учебы сотрудников;
-карточка унифицированной формы Т-2, утвержденная постановлением Госкомстатом России от 05.01.04 №1;
- другие документы, согласно законодательства Российской Федерации.

2.8. В целях информационного обеспечения Оператором могут создаваться общедоступные источники персональных данных работника (в том числе справочник электронные базы). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, должность, подразделение, служебные телефоны и адрес электронной почты.

2.9. 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, областных и муниципальных органов управления, страховые компании. Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции.

III. Хранение и защита персональных данных субъектов персональных данных

3.1. Персональные данные субъектов хранятся на бумажных носителях в помещении отдела кадров (регистратуре). Для этого используются специально оборудованные шкафы и сейфы. Личные дела уволенных (прошедших обследование, лечение) субъектов хранятся в архиве учреждения здравоохранения.

3.2. Сведения о начислении и выплате заработной платы субъектам учреждения здравоохранения хранятся на бумажных носителях в помещении управления экономики и бухгалтерского учета.

3.3. Конкретные обязанности по ведению, хранению личных дел субъектов, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные субъектов, возлагается на работников отдела кадров, а по хранению личных дел уволенных (обследованных, пролеченных) субъектов - на работников архива и закрепляются в должностных инструкциях. Обязательства по ведению, хранению, заполнению амбулаторных карт пациентов, историй болезней - на регистраторов, врачей, медицинских сестер.

3.4. 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. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.
3.5. Сведения о субъектах ПД учреждения здравоохранения хранятся также в электронном виде - в базах данных «МИС БАРС», «Парус» и других информационных системах.
3.6. При получении сведений, составляющих персональные данные субъектов, заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.
3.7. Защита информации о персональных данных.
3.7.1. Сотрудники МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону», имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.
3.7.2. На рабочих места сотрудников МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону», имеющие доступ к персональным данным, при пользовании доступом в сеть Интернет, должны быть приняты максимальные меры по обеспечению безопасности:
- установлено и использовано антивирусное ПО (с обновлением баз вирусов);
-установлен и использован брандмауэр;
- устанавливаться обновление для операционной системы.
3.7.3. За обеспечение безопасности персональных данных при их обработке, хранении и передаче ответственность несут следующие должностные лица МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону»:
- главный врач;
-заместители главного врача;
- главный бухгалтер;
- заместитель главного бухгалтера;
- начальник отдела кадров;
- специалисты отдела кадров (ведение трудовых книжек, личных карточек формы Т-2, личных дел);
- специалисты бухгалтерии (ведение документации по учету труда и его оплате);
- специалисты экономической службы;
- инженеры по охране труда;
- программисты;
- сотрудников отдела статистики;
- председатель профсоюзного комитета;
- руководители структурных подразделений;
- старшие медицинские сестры отделений;
-врачи и средний медицинский персонал;
- кассир отделения платных медицинских услуг;
-администраторы.

IV. Передача персональных данных субъектов ПД

4.1. При передаче персональных данных субъектов сотрудники МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону», имеющие доступ к персональным данным, должны соблюдать следующие требования:
4.1.1. Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных Трудовым Кодексом РФ, Основами законодательства об охране здоровья граждан или иными федеральными законами. Учитывая, что Трудовой кодекс РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью субъекта, оператор в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на предоставление его персональных сведений, либо, по мнению оператора, отсутствует угроза жизни или здоровью
субъекта, оператор обязан отказать в предоставлении персональных данных лицу.
4.1.2. Не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия.

4.1.3. 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.
4.1.4. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.
4.1.5. Все сведения об обращениях субъекта регистрируются в Журнале учета обращений субъектов ПД по вопросам обработки их ПД в целях контроля правомерности использования данной информации лицами, ее получившими.
4.1.6. Передавать персональные данные субъекта представителю субъекта в порядке, установленном Трудовым кодексом РФ и настоящим Положением, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанным представителем его функций.
4.2. Требования п.4.1. Положения не подлежат изменению, исключению, так как являются обязательными для сторон трудовых отношений на основании ст. 88 ТК РФ.

V. Обязанности субъекта и оператора ПД

5.1. В целях обеспечения достоверности персональных данных субъект обязан:
5.1.1. При приеме на работу (к врачу) предоставить оператору полные достоверные данные о себе.
5.1.2. В случае изменения сведений, составляющих персональные данные, субъект незамедлительно должен предоставить данную информацию оператору (учреждению здравоохранения).
5.2. Оператор обязан:
5.2.1. Осуществлять защиту персональных данных субъектов.
5.2.2. Обеспечить хранение первичной учетной документации по учету труда и его оплаты, к которой в частности, относятся документы по учету кадров, документы по учету использования рабочего времени и расчетов с субъектом по оплате труда, медицинская документация и др. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.
5.2.3. Заполнение документации, содержащей персональные данные работника, осуществлять в соответствии с унифицированными формами первичной учетной документации по учету труда и его оплаты, утвержденными постановлением Госкомстата России от 05.01.04 №1.
5.2.4. По письменному заявлению субъекта не позднее трех рабочих дней со дня подачи этого заявления выдать копии документов, связанных с работой и учебой (копии приказа о приеме на работу, приказов о переводах, приказа об увольнении с работы); выписки из трудовой книжки; справки о заработной плате, о начисленных и фактически уплаченных страховых взносах на обязательное пенсионное страхование, о периоде работы у данного оператора и другие. Копии документов, связанных с работой или учебой, должны быть заверены надлежащим образом и предоставляться субъекту безвозмездно.
5.2.5. Субъекты 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.
5.2.6. Все сотрудники Оператора, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных представлена в приложении № 4 настоящего положения.

VI. Права субъектов в целях защиты персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся у оператора, субъекты имеют право на:
6.1.1. Полную и безвозмездную информацию об их персональных данных и обработке этих данных.
6.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законом.
6.1.3. Определение своих представителей для защиты своих персональных данных.
6.1.4. Требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе оператора исключить или исправить персональные данные субъекта он имеет право заявить в

письменной форме оператору о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.
6.1.5. Требование об извещении оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведенных в них исключениях, исправлениях или дополнениях.
6.1.6. Обжалование в суд любых неправомерных действий или бездействия оператора при обработке и защите его персональных данных.

VII. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.
7.2. Разглашение персональных данных (передача их посторонним лицам, в том числе, сотрудникам администрации, не имеющим к ним доступа), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъектов, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим ПОЛОЖЕНИЕМ, локальными нормативными актами (приказами, распоряжениями) администрации, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарной ответственности.

VIII. Заключительные положения

8.1. Настоящее Положение вступает в силу с момента его утверждения главным врачом медицинского учреждения.
8.2. Настоящее Положение доводится до сведения всех работников медицинского учреждения.

Приложение 1
Форма заявления
о согласии работника
на обработку персональных данных

СОГЛАСИЕ
на обработку персональных данных

г. Ростов-на-Дону «__» _____ 20___г.

Я, _____
(фамилия, имя, отчество)

(далее Субъект), разрешаю МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону», в лице ответственных за обработку персональных данных должностных лиц (далее Оператору), обработку своих персональных данных (Список приведен в п.3 настоящего Согласия) на следующих условиях:

1. Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение следующих действий: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в ФЗ №152 от 27.07.2006 г., а также право на передачу такой информации третьим лицам, если это необходимо для поддержания функционирования информационных систем обеспечения и мониторинга учебного процесса, хозяйственной, научной, организационной и финансово-экономической деятельности учреждения здравоохранения и в случаях, установленных нормативными документами вышестоящих органов и законодательством.

2.Оператор обязуется использовать данные Субъекта для функционирования информационных систем обеспечения и мониторинга учебного процесса, хозяйственной, научной, организационной и финансово-экономической деятельности учреждения здравоохранения в соответствии с действующим законодательством Российской Федерации. Оператор может раскрыть государственным органам любую информацию по официальному запросу в случаях,установленных законодательством в стране проживания Субъекта.

3. Перечень персональных данных, передаваемых Оператору на обработку:

- Биографические сведения:
- Фамилия, имя, отчество, пол, дата и место рождения, гражданство;
- владение иностранным языком;
- специальность, квалификация;
- Сведения о местах обучения, образовании, ученой степени и ученом звании: (город, образовательное учреждение, сроки обучения):
- научные труды, изобретения, открытия, патенты, авторские свидетельства и др.;
- пребывание за границей;
- воинская обязанность;
- Сведения о местах работы, профессии, должности, стаже работы (город, название организации, должность, сроки работы);
- Сведения о наградах, поощрениях, взысканиях;
- Сведения о родителях, семейном положении, детях;
- Сведения о месте регистрации, проживания;
- Сведения о доходах, информации о выплатах и удержаниях;
- Сведения о социальных льготах,
- Паспортные данные;
- Данные документов об образовании, степенях, званиях, наградах, льготах, и др.;
- Номер страхового свидетельства государственного пенсионного страхования;

Индивидуальный налоговый номер (ИНН);

- Сведения о состоянии здоровья;
- Национальность (в случае указания субъекта);
- Фотографическое изображение.

4. Субъект дает согласие на включение в общедоступные источники персональных данных (в соответствии с п. 1 ст. 8 ФЗ №152 от 27.07.2006 г.) этой информации в рамках функционирования информационных систем обеспечения и мониторинга учебного процесса, научной, организационной и финансово-экономической деятельности учреждения здравоохранения, следующие персональные данные:
- Биографические сведения;
- Сведения о местах обучения, специальности, квалификации, ученой степени, ученом звании -город, образовательное учреждение, сроки обучения);
- Сведения о местах работы профессии, должности, стаже, наградах, льготах (город, название организации, должность, сроки работы);
- Фамилия, имя, отчество, пол, дата и место рождения;
- Адрес регистрации, адрес проживания;
- Сведения об области научных интересов, научных трудах, изобретениях, патентах, авторских свидетельствах и др.;
- Фотографическое изображение

5. Субъект персональных данных ознакомлен с документами организации, устанавливающими порядок обработки персональных данных, а так же со своими правами и обязанностями в этой области. Субъект персональных данных по письменному запросу имеет право на получение информации, касающейся обработки его персональных данных (в соответствии с п. 4 ст. 14 ФЗ №152 от 27.07.2006 г.)

6. Обработка персональных данных, не включенных в общедоступные источники, прекращается по истечении трёх лет с даты увольнения работника, за исключением случаев передачи данных на архивное хранение. Данные удаляются (уничтожаются) из информационных систем учреждения здравоохранения после указанного срока.

6.1. При поступлении Оператору письменного заявления Субъекта о прекращении действия Согласия в случае увольнения, персональные данные деперсонализируются в 15-дневный срок.

7. Настоящее согласие действует в течение срока хранения личного дела субъекта.

8. Подтверждаю, что ознакомлен с Положением о персональных данных, права и обязанности в области защиты персональных данных мне разъяснены.

_____	_____	_____
(дата)	(подпись)	(расшифровка подписи)

Приложение 2
Форма разработана согласно
Федеральному закону №152-ФЗ
"О персональных данных"
от 27 июля 2006г.

СОГЛАСИЕ ПАЦИЕНТА НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ МБУЗ «ГОРОДСКАЯ ПОЛИКЛИНИКА №12 Г. РОСТОВА-НА-ДОНУ»

Я _____, действующая(ий) в инте
(ФИО (полностью)
ресах несовершеннолетнего _____
(Ф.И.О. полностью)
Проживающ(ая)ий по адресу: _____,
(место регистрации)

паспорт _____, выдан _____,
(серия и номер) (дата, название выдавшего органа)

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 «О персональных данных» № 152-ФЗ в целях оказания мне медицинских услуг подтверждаю свое согласие на обработку МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» (далее - Оператор) моих персональных данных, а именно: фамилия, имя, отчество; пол,дата рождения, адрес места жительства, телефон, место работы, данные паспорта (или иного документа удостоверяющего личность), данные полиса ОМС (или ДМС); страховой номер индивидуального лицевого счета (СНИЛС), сведения о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью; сведения о диагностических мероприятиях, назначенном и проведённом лечении, данных рекомендациях.

В соответствии с требованиями статьи 10 Федерального закона от 27.07.2006 «О персональных данных» № 152-ФЗ даю согласие на обработку моих персональных данных Оператором при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

Оператор имеет право:

- при обработке моих персональных данных вносить их в реестры, базы данных автоматизированных информационных систем для формирования отчётных форм и иных сведений, предоставление которых регламентировано договорами или иными документами, определяющими взаимодействие Оператора со страховыми медицинскими организациями, медицинскими организациями, органами управления здравоохранения, иными организациями;
- с целью выполнения своих обязательств, предусмотренных нормативными правовыми актами или договорами, на предоставление, передачу моих персональных данных иным организациям, при условии, что указанные предоставление передача будут осуществляться с использованием машинных носителей или по каналам связи с соблюдением мер, обеспечивающих защиту моих персональных данных от несанкционированного доступа, а также при условии, что их прием и обработка будут осуществляться лицом, обязанным сохранять профессиональную тайну.

Даю согласие на то, что срок хранения моих персональных данных соответствует сроку хранения медицинской карты и составляет двадцать пять лет. По истечении указанного срока хранения моих персональных данных Оператор обязан уничтожить все мои персональные данные, включая все копии на машинных носителях информации.

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

Я согласен (а) со следующими действиями с моими персональными данными:

1. Обработка моих персональных данных в защищённых в установленном порядке автоматизированных информационных системах персональных данных пациентов;
2. Обработка моих персональных данных, защищённых в установленном порядке, без использования средств автоматизации.

Я оставляю за собой право отозвать свое согласие полностью или частично по моей инициативе на основании личного письменного заявления, в т.ч. и в случае ставших мне известных фактов нарушения моих прав при обработке персональных данных. В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных Оператор обязан прекратить их обработку.

_____ «___»_____ 201__ г.
(подпись, Ф.И.О.) (дата)

Согласие получено «__»_____ 201_ г.
(дата)

Уполномоченный представитель медицинской организации _____
(подпись)

Приложение 3
Форма заявления
об отказе на обработку
персональных данных

МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону»
Наименование (Ф.И.О.) оператора
Адрес оператора

Ф.И.О. субъекта персональных данных
Адрес, где зарегистрирован субъект
персональных данных
Номер основного документа, удостоверяющего
его личность
Дата выдачи указанного документа
Наименование органа, выдавшего документ

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с неправомерным их использованием.

«__» _____2018 г.

Приложение 4
Форма заявления о
неразглашении персональных
данных субъекта

СОГЛАШЕНИЕ

о неразглашении персональных данных субъекта

Я,_____, паспорт серии_____, номер _____,
выданный_____

"___"_____года, понимаю, что получаю доступ к персональным данным работников и/или пациентов МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону». Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

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

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в "Положении об обработке и защите персональных данных работников и пациентов МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону».

Я подтверждаю, что не имею права разглашать сведения:

- биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- состояние здоровья;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики;
- прочие сведения.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового кодекса Российской Федерации и ст. 183 Уголовного кодекса РФ.

_____ _____ _____
(дата) (подпись) (расшифровка подписи)

Приложение № 2
к приказу МБУЗ «Городская
поликлиника №12 г Ростова-на-Дону»
от 14.08.18 №132

Инструкция
по порядку учета и хранению съемных носителей конфиденциальной информации (персональных данных) в МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону»

1. Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации, предоставляемых органом исполнительной власти (далее наименование ОИВ) для использования в информационной системе.
1.2. Действие настоящей Инструкции распространяется на работников МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» (далее-Учреждение), подрядчиков и третью сторону.

2. Основные термины, сокращения и определения

1. **Администратор ИС** – технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
2. **АРМ** – автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
3. **ИБ** – информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.
4. **ИС** – информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.
5. **Носитель информации** – любой материальный объект, используемый для хранения и передачи электронной информации.
6. **Паспорт ПК** – документ, содержащий полный перечень оборудования и программного обеспечения АРМ.
7. **ПК** – персональный компьютер.
8. **ПО** – Программное обеспечение вычислительной техники.
9. **ПО вредоносное** – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
10. **ПО коммерческое** – ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
11. **Пользователь** – работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования носителей информации

3.1. Под использованием носителей информации в ИС Учреждения понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.
3.2. В ИС допускается использование только учтенных носителей информации, которые являются собственностью Учреждена и подвергаются регулярной ревизии и контролю.

3.3. К предоставленным Учреждению носителям конфиденциальной информации предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. Носители конфиденциальной информации предоставляются сотрудникам организации по инициативе руководителей структурных подразделений в случаях:

-необходимости выполнения вновь принятым работником своих должностных обязанностей;

-возникновения у сотрудника организации производственной необходимости.

4. Порядок учета, хранения и обращения со съемными носителями конфиденциальной информации (персональных данных), твердыми копиями и их утилизации.

4.1. Все находящиеся на хранении и в обращении съемные носители с конфиденциальной информацией (персональными данными) в Учреждении подлежат учёту.

4.2. Каждый съемный носитель с записанными на нем конфиденциальной информацией (персональными данными) должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.3. Учет и выдачу съемных носителей конфиденциальной информации (персональных данных) осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в журнале учета съемных носителей конфиденциальной информации.

5. При использовании работниками носителей конфиденциальной информации необходимо:

5.1. Соблюдать требования настоящего Положения;

5.2. Использовать носители информации исключительно для выполнения своих служебных обязанностей;

5.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящей Инструкции;

5.4. Бережно относится к носителям конфиденциальной информации;

5.5. Обеспечивать физическую безопасность носителей информации всеми разумными способами;

5.6. Извещать администраторов ИС о фактах утраты (кражи) носителей конфиденциальной информации.

6. При использовании носителей конфиденциальной информации запрещено:

6.1. Использовать носители конфиденциальной информации в личных целях:

6.2. Передавать носители конфиденциальной информации другим лицам (за исключением администраторов ИС);

6.3. Хранить съемные носители с конфиденциальной информацией (персональными данными) вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

6.4 Выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

7. Ответственность

7.1. Работники, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством и локальными нормативными актами организации.

Приложение № 3

к приказу МБУЗ «Городская поликлиника №12 г Ростова-на-Дону»

от 28.08.18 №152

ИНСТРУКЦИЯ
по порядку учета и хранению документов, содержащих персональные данные, в МБУЗ «городская поликлиника №12 г. Ростова-на-Дону»

1. Общие положения

1.1.Настоящая Инструкция разработана с целью обеспечения безопасности персональных данных при работе с документами, содержащими персональные данные.

1.2.Действие настоящей Инструкции распространяется на сотрудников МБУЗ «городская поликлиника №12 г. Ростова-на-Дону» (далее – Учреждение), допущенных к обработке персональных данных.

2. Порядок учета, хранения и обращения с документами, которые содержат персональные данные

2.1.Все находящиеся на хранении и в обращении документы с персональными данными в Учреждении подлежат учёту.

2.2.Каждый документ, личное дело или журнал должны иметь уникальный учетный номер.

2.3.Учет и выдачу документов с персональными данными осуществляют сотрудники структурных подразделений, на которых возложены функции хранения документов, содержащих персональные данные. Факт выдачи документов фиксируется в журнале учета.

2.4.При работе с документами, которые содержат персональные данные необходимо:

- Соблюдать требования настоящей Инструкции.
-Использовать полученные документы исключительно для выполнения своих служебных обязанностей.
-Ставить в известность ответственного за обработку персональных данных о любых фактах нарушения требований настоящей Инструкции.
-Бережно относится к документам, содержащим персональные данные.
-Обеспечивать физическую безопасность документов всеми разумными способами.
-Обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях
-Извещать ответственного за организацию обработки персональных данных о фактах утраты (кражи) документов, содержащих персональные данные.
-Осуществлять вынос документов с персональными данными для непосредственной передачи адресату только с письменного разрешения руководителя.

-При передаче персональных данных передаётся минимальный объем данных, который необходим для выполнения служебных обязанностей адресата.
-В случае утраты или уничтожения документов, которые содержат персональные данные либо разглашении содержащихся в них сведений, немедленно ставится в известность руководитель Учреждении. Отметки об утрате вносятся в журнал учета документов с персональными данными.
-В случае увольнения или перевода работника в другое структурное подразделение, предоставленные документы с персональными данными информации изымаются.

3. **Работа с журналом регистрации посетителей**

3.1.Журнал регистрации посетителей необходим исключительно в целях контроля посещаемости.
3.2.В Журнале учёта посещаемости разрешается фиксация следующих персональных данных:

- Фамилия, Имя, Отчество;
- Наименование и номер документа, удостоверяющего личность (паспорт, водительское удостоверение, удостоверение личности и т.д.);

3.3. Порядок учёта, хранения и обращения с журналом регистрации посетителей осуществляется в соответствии с п. 2 настоящей инструкции.
3.4. В случае окончания журнала, его необходимо сдать в архив или уничтожить.

4.Запрещается

4.1.Использовать документы с персональными данными в личных целях.
4.2.Передавать документы с персональными данными третьим лицам без соответствующего разрешения руководителя Учреждении.
4.3.Хранить документы с персональными данными вместе с документами с открытой информацией на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам.
4.4.Выносить документы с персональными данными из служебных помещений для работы с ними на дому и т. д.
4.5.Оставлять документы с персональными данными без присмотра.
4.6.Изготавливать и хранить копии паспортов или иных документов, удостоверяющих личность, за исключением случаев, предусмотренных законодательством.

5. Ответственность

5.1.Работники, нарушившие требования данной Инструкции, несут ответственность в соответствии с действующим законодательством.

Приложение № 4
к приказу МБУЗ «Городская
поликлиника №12 г Ростова-на-Дону»
от 15.08.18 №132

ИНСТРУКЦИЯ

Пользователя информационных систем персональных данных по обеспечению безопасности персональных данных в муниципальном бюджетном учреждении здравоохранения «Городская поликлиника №12 г. Ростова-на-Дону»

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных в муниципальном бюджетном учреждении здравоохранения «Городская поликлиника №12 г. Ростова-на-Дону» (далее - Учреждение).
1.2. Пользователем является каждый работник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
1.3. Пользователь несет персональную ответственность за свои действия.
1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о защите персональных данных и другими регламентирующими документами Учреждения.

2. Обязанности пользователя

Пользователь обязан:
2.1. Знать и выполнять требования настоящей Инструкции и других внутренних распоряжений, регламентирующих порядок действий по защите персональных данных.
2.2. Выполнять на автоматизированном рабочем месте (далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.
2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов.
2.4. Соблюдать требования парольной политики (раздел 3).
2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).
2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами, шторы на проемах должны быть завешаны (жалюзи закрыты)
2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а также для получения консультаций по вопросам информационной безопасности необходимо обратиться к Администратору информационной системы персональных данных или ответственному за обработку персональных данных.
2.8. Пользователям запрещается:
- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
-самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и

аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
-несанкционированно открывать общий доступ к папкам на своей рабочей станции;
-отключать (блокировать) средства защиты информации;
-обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе персональных данных;
-сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системы персональных данных;
-привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с ответственным за организацию работы с персональными данными.
2.9. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <CtrlxAlt><Del> и выбрать опцию <Блокировка>.
2.10. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

3. Организация парольной защиты

3.1. Полная плановая смена паролей в информационной системе персональных данных проводится не реже одного раза в 3 месяца.
3.2. Правила формирования пароля:
пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
пароль должен состоять не менее чем из 8 символов;
в пароле должны присутствовать символы трех категорий из числа следующих четырех:
а) прописные буквы английского алфавита от A до Z;
б) строчные буквы английского алфавита от a до z;
в) десятичные цифры (от 0 до 9);
г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);
запрещается использовать в качестве пароля имя входа в систему, простые пароли типа "123", "111", "qwerty" и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
запрещается выбирать пароли, которые уже использовались ранее.
3.3. Правила ввода пароля:
ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).
3.4. Правила хранения пароля:
запрещается записывать пароли на бумаге, в файле, в электронной записной книжке и на других носителях информации, в том числе на предметах;
запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
3.5. Лица, использующие паролирование, обязаны:
четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
своевременно сообщать ответственным за организацию работы с ПД об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети "Интернет" и других) (далее - Сеть) на элементах информационной системы персональных данных должна проводиться при служебной необходимости.
4.2. При работе в Сети запрещается:
- осуществлять работу при отключенных средствах защиты (антивирусах и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- посещать сайты сомнительной репутации.

Приложение № 5
к приказу МБУЗ «Городская
поликлиника №12 г Ростова-на-Дону»
от 17.08.18 №132

ПОРЯДОК

доступа сотрудников МБУЗ «Городская поликлиника №12 г Ростова-на-Дону» в помещения, в которых ведется обработка персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Порядок доступа сотрудников МБУЗ «Городская поликлиника №12 г Ростова-на-Дону» в помещения, в которых ведется обработка персональных данных (далее – Порядок) разработан в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства РФ от 01.11.2012 № 1119 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», в целях обеспечения защиты конфиденциальной информации, обрабатываемой в МБУЗ «Городская поликлиника №12 г Ростова-на-Дону», и исключения фактов неконтролируемого пребывания в них посторонних лиц. Настоящим документом определяются порядок доступа работников и посетителей в помещения, в которых ведется обработка персональных данных, а также правила обработки и хранения документов, содержащих персональные данные, и материальных носителей персональных данных.

Порядок устанавливает единые требования к обеспечению сохранности технических средств и персональных данных.

1. Доступ работников МБУЗ «Городская поликлиника №12 г Ростова-на-Дону» (далее – Организация) в помещения, в которых ведется обработка персональных данных, осуществляется в целях обеспечения безопасности персональных данных.

2. Для помещений, в которых обрабатываются персональные данные (далее – Помещения), должен обеспечиваться режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этом помещении посторонних лиц.

3. Право самостоятельного входа в Помещения имеют работники, непосредственно работающие в этих помещениях и лицо, ответственное за организацию обработки персональных данных.

4. Иные лица допускаются в Помещения по согласованию с руководством Организации или лицом, ответственным за организацию обработки персональных данных, и в сопровождении лиц, работающих в этих Помещениях.

5. Помещения по окончании рабочего дня должны закрываться на ключ.

6. Вскрытие и закрытие Помещений производится лицами, имеющими право доступа.

7. Уборка Помещений должна производиться в присутствии лиц, осуществляющих обработку персональных данных.

8. Перед закрытием Помещений по окончании рабочего дня, лица, имеющие право доступа в помещения, обязаны:

– убрать материальные носители персональных данных в шкафы или сейфы и закрыть их;

– отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

– закрыть окна.

9. Перед открытием Помещений лица, имеющие право доступа в помещения, обязаны:

– провести внешний осмотр с целью установления целостности двери и замка;

– открыть дверь и осмотреть Помещение, где хранятся материальные носители.

10. При обнаружении неисправности двери и запирающих устройств необходимо:

– не вскрывая Помещение, доложить непосредственному руководителю;

– в присутствии лица, ответственного за организацию обработки персональных данных, и непосредственного руководителя, вскрыть Помещение и осмотреть его;

– составить акт о выявленных нарушениях и передать его заведующей Организации для проведения служебного расследования.

11. Ответственность за соблюдение порядка доступа в Помещения возлагается на лицо, ответственное за организацию обработки персональных данных.

12. Работники Организации, должны ознакомиться с настоящим порядком доступа в помещения, в которых ведется обработка персональных данных, под подпись.

Приложение № 6
к приказу МБУЗ «Городская поликлиника №12 г Ростова-на-Дону»
от 29.08.18 №132

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону»

1. Общие положения

1.1 Настоящая инструкция разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказа ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных»

1.2 Настоящая инструкция определяет требования к организации защиты информационных систем персональных данных МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников, эксплуатирующих и сопровождающих информационные системы и программное обеспечение, за их выполнение.

1.3 К использованию в МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.4 Установка средств антивирусного контроля на компьютерах осуществляется Администратором безопасности системы передачи данных. Настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1 Ежедневно в начале работы при загрузке компьютера в автоматическом

режиме должен проводиться антивирусный контроль системных файлов.

2.2 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (DVD (CD)-ROM, flash-накопители и т. п.).

2.3 Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера.

2.4 Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.5 Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.6 Установка (изменение) системного и прикладного программного обеспечения осуществляется на основании заявки начальника отдела. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено Администратором безопасности информационной системы на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера на автоматизированном рабочем месте (АРМ) Администратором безопасности информационной системы должна быть выполнена антивирусная проверка.

2.7 Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в электронном журнале антивирусного средства (операционной системы).

2.8 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.) сотрудник самостоятельно или вместе с Администратором безопасности информационной системы должен провести внеочередной антивирусный контроль своей рабочей станции. При необходимости привлечь специалистов для определения ими факта наличия или

отсутствия компьютерного вируса.

2.9 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники обязаны:

– приостановить работу;
– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего руководителя и Администратора безопасности информационной системы, владельца зараженных файлов, а также других сотрудников, использующих эти файлы в работе;
– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
– провести лечение или уничтожение зараженных файлов;
– в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл на отдельном съемном носители Администратору безопасности информационной системы;
– по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору безопасности информационной системы, в которой необходимо указать предположительный источник (отправителя, владельца и т. д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

3.1 Ответственность за организацию антивирусного контроля в МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» и соблюдение требований настоящей инструкции возлагается на Администратора безопасности информационной системы.

3.2 Периодический контроль над состоянием антивирусной защиты в ИС, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции сотрудниками МБУЗ «Городская поликлиника №12 г. Ростова-на-Дону» осуществляется Администратором безопасности информационной системы.

Приложение № 7

к приказу МБУЗ «Городская
поликлиника №12 г Ростова-на-Дону»

от 14.08.18 №132

Список должностей МБУЗ «городская поликлиника №12 г. Ростова-на-Дону», имеющих доступ к персональным данным

- главный врач;
- заместители главного врача;
- главный бухгалтер;
- заместитель заместитель главного бухгалтера;
- начальник отдела кадров;
- специалисты отдела кадров (ведение трудовых книжек, личных карточек формы Т-2, личных дел);
- специалисты бухгалтерии (ведение документации по учету труда и его оплате);
- специалисты экономической службы;
- инженеры по охране труда;
- программисты;
- сотрудников отдела статистики;
- председатель профсоюзного комитета;
- руководители структурных подразделений;
- старшие медицинские сестры отделений;
- врачи и средний медицинский персонал;
- кассир отделения платных медицинских услуг;
- администраторы.