Муниципальное бюджетное учреждение здравоохранения
«Городская больница № 1»

УТВЕРЖДАЮ
Главный врач МБУЗ ГБ №1

_____ А.С.Трусов
«___»_____20___г.

ПОЛОЖЕНИЕ
о защите персональных данных работников МБУЗ «Городская больница №1»

1.Общие положения

1.1. Целью данного Положения является защита персональных данных работников МБУЗ «Городская больница №1» (далее МБУЗ ГБ №1) от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение устанавливает порядок обработки, приема, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, учета документов, содержащих сведения, отнесенные к персональным данным работников МБУЗ ГБ №1 с использованием средств автоматизации или без использования таких средств.

1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ от 30.12.2001 № 197-ФЗ, Федеральным законом РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Приказом Роскомнадзора России от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»; Приказом Министерства здравоохранения РО № 633-л от 29.11.2012 « Об утверждении правил обработки персональных данных работников министерства здравоохранения РО» и другими нормативными правовыми актами.

1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.5. Настоящее Положение утверждается и вводится в действие приказом главного врача МБУЗ ГБ №1 и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным работников учреждения. Все работники учреждения должны быть ознакомлены под роспись с данным положением и изменениями к нему.

2. Основные понятия и состав персональных данных

2.1. Основные понятия:

- ***персональные данные*** — любая информация, относящаяся к прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), являющемуся работником МБУЗ ГБ№1;

- ***Работники (сотрудники)*** — лица, имеющие трудовые отношения с учреждением, либо кандидаты на вакантную должность, вступившие с учреждением в отношения по поводу приема на работу.
- ***оператор*** — юридическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- ***обработка персональных данных*** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таки 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;
- ***автоматизированная обработка персональных данных*** – обработка персональных данных с помощью средств вычислительной техники;
- ***распространение персональных данных*** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- ***блокирование персональных данных*** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных;
- ***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;
- ***обезличивание персональных данных*** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- ***информационная система персональных данных*** — совокупность, содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
- ***трансграничная передача персональных данных*** – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
- ***конфиденциальность персональных данных*** — обязательное для соблюдения работодателем (оператором) или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия сотрудника или наличия иного законного основания;

2.2. В состав персональных данных работника входят:

- анкетные и биографические данные (фамилия, имя, отчество; год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности работника);
- образование (данные об образовании работника, наличии специальных знаний или подготовки);
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- данные о профессии, специальности работника;

- занимаемая должность;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т-2) и трудовые книжки работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- анкеты, заполняемые работниками;
- сведения о доходах работника;
- данные, содержащиеся в трудовой книжке работника и его личном деле, страховом свидетельстве государственного пенсионного страхования, свидетельстве о постановке на налоговый учет;
- данные, содержащиеся в документах воинского учета (при их наличии);
- документы о состоянии здоровья работника;
- иные персональные данные, при определении объема и содержания которых работодатель (оператор) руководствуется настоящим Положением и законодательством РФ.

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

3. Создание, обработка и хранение персональных данных работника

- 3.1. Создание персональных данных работника.
- Документы, содержащие персональные данные работника, создаются путем:
- а) копирования оригиналов (документ об образовании, свидетельство ИНН, пенсионное свидетельство);
- б) внесения сведений в учетные формы (на бумажных и электронных носителях);
- в) получения оригиналов необходимых документов (трудовая книжка, личный листок по учету кадров, автобиография, медицинское заключение).
- г) получение от третьих лиц
- 3.2. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.
- 3.2.1. При обработке персональных данных работника в целях их защиты и обеспечения прав и свобод человека и гражданина, а также при определении объема и содержания обрабатываемых персональных данных должны строго учитываться положения Конституции Российской Федерации, Трудового кодекса Российской Федерации и иных федеральных законов.
- 3.2.2. Обработка персональных данных работника осуществляется исключительно в целях:
- а) обеспечения соблюдения законов и иных нормативных правовых актов;
- б) содействия работникам в трудоустройстве;
- в) обеспечения личной безопасности работников;
- г) контроля количества и качества выполняемой работы;
- д) обеспечения сохранности имущества работника и работодателя(оператора).
- 3.2.3. Все персональные данные работника следует получать у него самого, за исключением случаев, если их получение возможно только у третьей стороны.
- 3.2.4. Получение персональных данных работника у третьих лиц возможно только при уведомлении работника об этом заранее и с его письменного согласия.

- В уведомлении работника о получении его персональных данных у третьих лиц должна содержаться следующая информация:
- а) о целях получения персональных данных;
- б) о предполагаемых источниках и способах получения персональных данных;
- в) о характере подлежащих получению персональных данных;
- г) о последствиях отказа работника дать письменное согласие на их получение.
- 3.2.5. Работодатель (оператор) не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, равно как и персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
- 3.2.6. При принятии решений, затрагивающих интересы работника, работодатель (оператор) не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.
- 3.2.7. Работники и их представители должны быть ознакомлены под расписку с документами работодателя(оператора), устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
- 3.3. Сведения, содержащие персональные данные работника, включаются в его личное дело, карточку формы N Т-2, а также содержатся на электронных носителях информации, доступ к которым разрешен лицам, непосредственно использующим персональные данные работника в служебных целях и согласия работника. С письменного согласия работника в ОК могут храниться копии его личных документов (паспорт; СНИЛС; ИНН; военный билет; свидетельство о рождении детей; Свидетельство о заключении брака и расторжении; диплом, иные документы об образовании, повышении квалификации и тд.)
- 3.4. Хранение персональных данных в бухгалтерии:
- а) персональные данные, содержащиеся на бумажных носителях, хранятся в запираемом шкафу, установленном на рабочем месте главного бухгалтера;
- б) персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК главного бухгалтера.
- 3.4.1. Персональные данные, включенные в состав личных дел, хранятся в запираемом шкафу, установленном на рабочем месте инспектора по кадрам. Персональные данные, содержащиеся на электронных носителях информации, хранятся в ПК инспектора по кадрам.
- 3.4.2. Трудовая книжка, документы воинского учета, карточка формы N Т-2 хранятся в запертом металлическом сейфе.
- 3.4.3. Доступ к ПК строго ограничен кругом лиц, определенных в п. 4.1 настоящего Положения. Персональные данные, содержащиеся на бумажных носителях, сдаются в архив после истечения установленного срока хранения.
- Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работника, определяются также должностными инструкциями.

4. Доступ к персональным данным

- 4.1. Внутренний доступ (доступ внутри организации).
- 4.1.1. Право доступа к персональным данным с согласия сотрудника имеют:
- - главный врач учреждения;
- -руководители структурных подразделений (отделений) по направлению деятельности (доступ к личным данным только работников своего подразделения (отделения));
- - при переводе из одного структурного подразделения (отделения) в другое доступ к

персональным данным работника может иметь руководитель нового подразделения(отделения);

- - сам работник, носитель данных;
- -другие сотрудники учреждения, назначенные для организации обработки персональных данных работников МБУЗ ГБ №1
- Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом главного врача учреждения.
- 4.2. Внешний доступ.
- 4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:
- - налоговые инспекции;
- - правоохранительные органы;
- - органы статистики;
- - страховые агентства;
- - военкоматы;
- - органы социального страхования;
- - пенсионные фонды;
- - подразделения муниципальных органов управления.
- 4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
- 4.2.3. Организации, в которые сотрудник может осуществлять перечисление денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.
- 4.2.4. Другие организации.
- Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника, в случае если он в этой (другой) организации работает.
- Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.
- В случае развода бывшая супруга (супруг) имеет право обратиться в учреждение с письменным запросом о размере заработной платы сотрудника без его согласия (ТК РФ).

5. Защита персональных данных

- 5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.
- 5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и не заинтересованные в возникновении угрозы лица.
- 5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности учреждения.
- 5.4. Защита персональных данных работника от неправомерного их использования или

утраты должна быть обеспечена работодателем(оператором) за счет его средств в порядке, установленном федеральным законом.

- **5.5. Внутренняя защита**

- 5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.
- 5.5.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:
- - ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- - строгое избирательное и обоснованное распределение документов и информации между работниками;
- - рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- - знание работником требований нормативно-методических документов по защите информации и сохранению тайны;
- - наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- - определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- - организация порядка уничтожения информации;
- - своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- - воспитательная и разъяснительная работа с сотрудниками подразделения(отделений) по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- - не допускается выдача личных дел работников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения(отделения) (например, при подготовке материалов для аттестации работника).
- 5.5.3. Защита персональных данных сотрудника на электронных носителях.
- Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается главному врачу и руководителю службы информационных технологий;
- Средствами антивирусной защиты;
- Средствами криптозащиты, сертифицированными Федеральной службой по техническому и экспортному контролю (ст.19 ФЗ-152 от 27.07.2006 ; Приказ ФСБ РФ от 10.07.2014 № 378; Постановление Правительства РФ от 01.11.2012 № 1119)
- 5.6. Внешняя защита.
- 5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

- 5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения (посетители, работники других организационных структур). Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.
- 5.6.3. Для обеспечения внешней защиты персональных данных работников необходимо соблюдать ряд мер:
- - порядок приема, учета и контроля деятельности посетителей;
- - пропускной режим учреждения;
- - технические средства охраны, сигнализации;
- - порядок охраны территории, зданий, помещений, транспортных средств;
- - требования к защите информации при интервьюировании и собеседованиях.
- 5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.
- 5.8. По возможности персональные данные обезличиваются.
- 5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатель(оператор), работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Право на обжалование действий или бездействия оператора

6.1.Если работник или его законный представитель считает, что Учреждение-оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Учреждения-оператора в уполномоченный орган по защите прав субъектов персональных данных (Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи) или в судебном порядке.

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

Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

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

- 7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной ответственности. К данным лицам могут быть применены следующие дисциплинарные взыскания:
- а) замечание;
- б) выговор;
- в) увольнение (ст.81 ТК РФ).
- А также лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут материальную, руководитель учреждения административную (ст.ст.5.27; 5.39 КоАП РФ), гражданско-правовую или уголовную ответственность (ст.188 УК РФ) в порядке, установленном федеральными законами.

- 7.2. Сотрудники, имеющие доступ к персональным данным работника и совершившие указанный дисциплинарный проступок, несут полную материальную ответственность в случае причинения его действиями ущерба работодателю (ст. 243 Трудового кодекса РФ).

- 7.3. За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

- 7.4. Копия приказа о применении к работнику дисциплинарного взыскания с указанием оснований его применения вручается работнику под расписку в течение пяти дней со дня издания приказа.

- 7.5. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Работодатель до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

Приложение №1
к Положению о защите персональных данных
работников МБУЗ «Городская больница № 1»

Главному врачу
МБУЗ «Городская больница № 1»
_____
Ф.и.о.
_____

(Ф.И.О. субъекта перс.данных или его представителя)

Паспорт :_____
(полные паспортные данные, для представителя субъекта перс.данных, указать дополнительно и реквизиты доверенности)

_____
Зарегистрированный по адресу:
_____

СОГЛАСИЕ
на обработку персональных данных

Я,_____ _____ (далее субъект персональных
Ф.и.о.
данных), проживающая (зарегистрирована) по адресу: _____
_____ _____, паспорт (иной основной документ, удостоверяющий личность) _____ в соответствии со ст. 9 ФЗ №152-ФЗ «О персональных данных» в своей воле и в своем интересе даю свое согласие главному врачу МБУЗ «Городская больница №1(далее Оператор) на обработку(любое действие или совокупность действий, включая сбор, запись, систематизацию , накопление, хранение, уточнение, извлечение(обновление, изменение), использование, распространение(в т.ч. передачу), обезличивание, блокирование, удаление, уничтожение моих персональных данных: _____ _____ (указать перечень обрабатываемых данных) сведения о факте обращения за медицинскими услугами, состоянии здоровья и заболеваниях, полученных в ходе оказания услуг, в целях оказания медицинских услуг и выполнения иных обязательств по договору, а также выполнения Оператором в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов при содействии в трудоустройстве, обучении, продвижении по работе, обеспечении личной моей безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества, в целях взаимодействия представления информации в государственные органы Российской Федерации в порядке, предусмотренным действующим законодательством.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу(субъекту персональных данных), указанная в трудовом договоре , личной карточке (ф Т-2), трудовой книжке и полученная в течение срока действия настоящего трудового договора, в том, числе: моя фамилия, имя, отчество , год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный

номер налогоплательщика (ИНН), номер страхового свидетельства государственного пенсионного страхования (СНИЛС), адрес фактического места проживания и регистрации по месту жительства, почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, семейном положении и составе семьи, сведения об имущественном положении, доходах, задолженности, занимаемых ранее должностях и стаже работы, воинской обязанности, сведения о трудовом договоре и его исполнении (занимаемы должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказании услуг и т.п.), заключаемых при исполнении трудового договора.

Своей волей и в своих интересах выражаю согласие на осуществление Оператором любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение(обновление, изменение), использование, распространение(в т.ч. передачу), обезличивание, блокирование, уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке; запись на электронные носители и их хранение; передачу Оператором по своему усмотрению данных и соответствующих документов, содержащих персональные данные, третьим лицам, корректного документального оформления трудовых правоотношений между мною и главным врачом; обеспечения выполнения мною должностных обязанностей; представления информации в государственные органы Российской Федерации в порядке, предусмотренным действующим законодательством; предоставления информации в медицинские учреждения , страховые компании; обеспечения предоставления мне социального пакета;
хранением моих персональных данных в течение 75 лет , содержащихся в документах, образующихся в деятельности главного врача, согласно части 1 стать 17 Закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации», а также при осуществлении любых иных действий с моими персональными данными указанными в трудовом договоре и полученными в течение срока действия трудового договора, в соответствии с требованиями действующего Законодательства РФ и Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при предоставлении Оператору заявления в простой письменной форме в соответствии с требования законодательства Российской Федерации.

Обязуюсь сообщать в трехдневный срок об изменении места жительства, контактных телефонов, паспортных данных, документных и иных персональных денных.

Об ответственности за достоверность представленных персональных сведений предупрежден(а).

Я подтверждаю что, давая такое Согласие, я действую своей волей и в своих интересах.

«_____»_____20___г. _____ /_____/

Приложение N 2 к Положению о защите персональных данных
работников МБУЗ «Городская больница № 1»

Обязательство о неразглашении персональных данных работников МБУЗ «Городская больница № 1»

Я, _____

Ф.и.о. ответ.сотрудника

с Положением о защите персональных данных работников МБУЗ «Городская больница № 1» ознакомлен(а). Обязуюсь не разглашать персональные данные работников, ставшие мне известными в связи с исполнением должностных обязанностей.

Об ответственности за разглашение персональных сведений работников предупрежден(а).

_____ "__" _____ ____ *г.*

Приложение N 3 к Положению о защите персональных данных работников МБУЗ «Городская больница № 1»

Главному врачу

_____

Ф.и.о.

от _____,
зарегистрированного по адресу
_____
паспорт _____

Я,_____, ознакомлен с Положением о защите персональных данных работников МБУЗ ГБ №1, мне разъяснены все мои права и обязанности.

Настоящим даю своё согласие о хранении в моем личном деле копий моих документов, в том числе: копии паспорта, копии СНИЛС;, ИНН; копии свидетельств: об образовании; повышении квалификации, о рождении детей; о регистрации и расторжении брака; копии диплома и других документов, в том числе выданных госорганами.

«_____»_____20____г. _____

Приложение N 4 к Положению о защите персональных данных работников МБУЗ «Городская больница № 1»

Главному врачу

_____

Ф.и.о.

от _____,
зарегистрированного по адресу
_____
паспорт _____

Согласие
на передачу персональных данных третьей стороне

Я, _____ в соответствии с абз. 1 ч. 1 ст. 88 ТК РФ; Федерального закона №152-ФЗ от 27.07.2006 «О персональных данных», даю согласие МБУЗ «Городская больница № 1», расположенной по адресу ул. Мацоты С.В. 28, на предоставление, в соответствии с действующим законодательством третьей стороне запрашиваемые в отношении меня персональные данные, перечень которых указан в Согласии на обработку персональных данных, явл. Приложением № 1 к настоящему Положению.

Настоящее согласие действительно до его отзыва, на период действия моих трудовых отношений с Оператором (работодателем). а также на период хранения моих персональных данных после окончания трудовых отношений в учреждении.

_____ "__" _____ ____ *г.*

Приложение N 5 к Положению о защите персональных данных работников МБУЗ «Городская больница № 1»

Главному врачу

_____

Ф.и.о.

от _____,
зарегистрированного по адресу
_____
паспорт _____

РАЗЪЯСНЕНИЯ
РАБОТНИКУ ЮРИДИЧЕСКИХ ПОСЛЕДСТВИЙ
ОТКАЗА ПРЕДОСТАВИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

_____
__,
(фамилия, имя, отчество)
_____
__
_____
__,
(должность, структурное подразделение министерства здравоохранения Ростовской области)

в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена
_____
_____
__
_____
__. (указываются реквизиты и наименования нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные министерство здравоохранения Ростовской области не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:
_____
_____
__
_____
__.
(перечисляются юридические последствия для работника)

В соответствии с действующим законодательством Российской Федерации в области персональных данных Вы имеете право: на получение сведений о министерстве здравоохранения Ростовской области (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения министерства здравоохранения Ростовской области, о наличии у министерства здравоохранения Ростовской области своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от министерства здравоохранения Ростовской области разъяснения порядка защиты своих прав и законных интересов; обжаловать действия или бездействие должностных лиц министерства здравоохранения Ростовской области в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Наименование должности
работника управления кадровой
и организационно-методической работы,
подготовившего разъяснения _____ _____

(подпись) (инициалы, фамилия)

Ознакомлен

_____ _____

(подпись) (расшифровка подписи)

«_____» _____ 20__ г.

Приложение № 4 к
Положению о защите персональных
данных работников МБУЗ
«Городская больница № от 2018 г.

Согласие работника на обработку персональных данных в соответствии с Федеральным законом от 30.12.2020 № 519-ФЗ

Главному врачу МБУЗ «Городская больница №1»
Трусову А.С.

от _____
(фамилия, имя, отчество)
зарегистрированного по адресу:
_____
(адрес регистрации указывается
_____
с почтовым индексом)
паспорт серия_____

_____
(дата выдачи органа, выдавшего документ)

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество полностью)

в соответствии с Федеральным законом от 30.12.2020 № 519-ФЗ и ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", в целях:
- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в кредитную организацию для оформления банковской карты и перечисления на нее заработной платы;
- предоставления сведений третьим лицам для оформления полиса ДМС;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности имущества работодателя даю согласие МБУЗ «Городская больница №1" расположенному по адресу: 346404, Ростовская область, г.Новочеркасск, ул. Мацоты С.В., д.28 на автоматизированную, а также без использования средств автоматизации обработку моих

персональных данных, а именно на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;
- пол, возраст;
- дата и место рождения;
- паспортные данные;
- адрес регистрации по месту жительства и адрес фактического проживания;
- номер телефона (домашний, мобильный);
- данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации;
- семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством;
- отношение к воинской обязанности;
- сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;
- СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в МБУЗ «Городская больница №1"
- сведения о доходах в МБУЗ «Городская больница № 1»;
- сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

_____ (подпись)

(расшифровка подписи)

_____ (дата)

МБУЗ «ГОРОДСКАЯ БОЛЬНИЦА№1»

П Р И К А З

____.____.20____ г. г. НОВОЧЕРКАССК № ____

Об утверждении правил обработки
персональных данных работников
МБУЗ «Городская больница № 1»

В соответствии с требованиями Трудового законодательства РФ; Федеральным законом РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных» и Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»»,

ПРИКАЗЫВАЮ:

1. Утвердить Правила обработки персональных данных работников и пациентов МБУЗ «Городская больница № 1», согласно приложению.
2. Начальнику ОК Казьминой Е.П. ознакомить под роспись всех ответственных лиц учреждения,
допущенных к обработке персональных данных.
3 Контроль за исполнением приказа оставляю за собой.

Главный врач А.С.Трусов

Приложение №1
к приказу от

_____№ ____

ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ
РАБОТНИКОВ МБУЗ «Городская больница № 1»

1. Общие положения

1.1. Правила обработки персональных данных работников и пациентов МБУЗ «Городская больница № 1» (далее - Правила) разработаны в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»
1.2. Настоящие Правила устанавливают процедуру обработки персональных данных работников и пациентов МБУЗ «Городская больница № 1».
1.3. Сбор, систематизацию, накопление, хранение, обновление, изменение, передачу, уничтожение и другое использование документов, содержащих персональные данные работников и пациентов МБУЗ «Городская больница № 1», осуществляют работники учреждения, закрепленные Приказом главного врача. Ответственность за обеспечение защиты персональных данных пациентов, обрабатываемых в отделениях, возлагается на заведующих отделений(поликлиник).
1.4. Организацию работы по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации, осуществляет отдел программно-информационного обеспечения учреждения.
Ответственность за организацию данной работы возлагается на начальника отдел программно-информационного обеспечения учреждения.
1.5. Сведения о фактах, событиях и обстоятельствах частной жизни работников и пациентов МБУЗ «Городская больница № 1», содержащиеся в документах, указанных в настоящих Правилах, а также персональные данные, внесенные в личные дела работников и истории болезни(карточки) пациентов МБУЗ «Городская больница № 1» и иные сведения, содержащиеся в личных делах работников и карточках пациентов, относятся к сведениям конфиденциального характера.

2. Перечень документов, содержащих персональные
данные работников и пациентов МБУЗ «Городская больница № 1», обрабатываемых в связи с реализацией трудовых отношений работников и получения пациентами медицинских услуг.

К документам, содержащим персональные данные работников МБУЗ «Городская больница № 1», подлежащие защите, относятся:
трудовые книжки;
личные дела медработников;
личные карточки (унифицированные формы первичной учетной документации N Т-2ГС (МС) и N Т-2);
справки-объективки;
книга учета движения трудовых книжек и вкладышей в них;

трудовые договоры работников, осуществляющих техническое обеспечение деятельности учреждения;
табель учета рабочего времени и расчета оплаты труда (унифицированная форма первичной учетной документации N Т-12);
расчетно-платежная ведомость, платежная ведомость;
карточка-справка (расчет заработной платы);
налоговая карточка по учету доходов и налога на доходы физических лиц (форма 1-НДФЛ);
справка о доходах физического лица (форма 2-НДФЛ);
формы документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования;
индивидуальная карточка учета сумм начисленных выплат и иных вознаграждений, сумм начисленного единого социального налога, страховых взносов на обязательное пенсионное страхование (налогового вычета);
индивидуальная карточка учета сумм начисленных выплат и иных вознаграждений, страховых взносов на обязательное пенсионное страхование;
свидетельство о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации.

К документам, содержащим персональные данные пациентов МБУЗ «Городская больница № 1», подлежащие защите, относятся все документы и их копии представляющие собой любую информацию, относящуюся к прямо или косвенно определенному или определяемому пациенту(физическому лицу, субъекту персональных данных)

3. Ведение личных дел

3.1. В личное дело работника вносятся его персональные данные и иные сведения, связанные с поступлением на работу в учреждение.
3.2. Ведение личных дел сотрудников осуществляют работники отдела кадров учреждения.
3.3.К личному делу сотрудника приобщаются :
письменное заявление с просьбой о поступлении на работу;
собственноручно заполненная и подписанная гражданином Российской Федерации анкета установленной формы с приложением фотографии;
копии приказов о поощрении сотрудника, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

К личному делу сотрудника приобщаются для хранения в деле с их письменного согласия:
копия паспорта и копии свидетельств о государственной регистрации актов гражданского состояния;
копия трудовой книжки или документа, подтверждающего прохождение военной или иной службы;
копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);
копии решений о награждении государственными наградами Российской Федерации ведомственными наградами(если таковые имеются);
копия страхового свидетельства обязательного пенсионного страхования;
копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;
копия страхового медицинского полиса обязательного медицинского страхования граждан;
3.4.К личному делу сотрудника приобщаются иные документы, предусмотренные федеральными законами и иными нормативными правовыми актами Российской Федерации.
3.5. Документы, приобщенные к личному делу сотрудника, брошюруются, страницы нумеруются, к личному делу прилагается опись.

Ведение карт пациентов:

4. Порядок обращения с документами
и другими носителями информации, содержащими
персональные данные, подлежащие защите

4.1. Все персональные данные должны быть получены непосредственно от работников учреждения, при этом их обработка осуществляется по письменному заявлению-согласию по форме согласно приложению №1 к настоящим Правилам.
В случае отказа работника предоставить свои персональные данные ему даются письменные разъяснения о юридических последствиях такого отказа по форме согласно приложению №2 к настоящим Правилам.
4.2. Прием и учет документов и других носителей информации, содержащих персональные данные, подлежащие защите, осуществляют работники отдела кадров.
4.3. При заключении трудового контракта с работником, непосредственно осуществляющим обработку персональных данных, он подписывает обязательство о неразглашении персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, по форме согласно приложению №3 к настоящим Правилам.
4.4. Личные дела работников и другие документы, содержащие персональные данные, подлежащие защите, выдаются начальником отдела кадров учреждения по карточке выдачи с распиской пользователей о получении и с распиской начальника отдела в обратном приеме документов.
4.5. Сведения, содержащиеся в документах, указанных в разделе 2 настоящих Правил, пересылаются сторонним организациям заказными или ценными почтовыми отправлениями, нарочным с письменным уведомлением.
4.6. Черновики и проекты документов уничтожаются путем сожжения или измельчения в бумагорезательной машине.
4.7. При смене работника, ответственного за учет документов и других носителей информации, содержащих персональные данные, подлежащие защите, составляется акт приема-сдачи этих материалов, который утверждается гл.врачом.

5. Обязанности должностных лиц по сохранению
персональных данных, подлежащих защите

5.1. При работе со сведениями, содержащими персональные данные, подлежащие защите, работники учреждения обязаны:
знакомиться только с теми документами, к которым получен доступ в соответствии со служебной необходимостью;
хранить в тайне ставшие известными им сведения, содержащие персональные данные, подлежащие защите, информировать непосредственного руководителя о фактах нарушения порядка обращения с персональными данными и о попытках несанкционированного доступа к ним;
о допущенных нарушениях установленного порядка работы, учета и хранения документов, а также о фактах разглашения сведений, содержащих персональные данные, подлежащие защите, представлять главному врачу(завотделения) письменные объяснения.
5.2. При работе со сведениями, содержащими персональные данные, подлежащие защите, запрещается:
работать на персональных компьютерах, не предназначенных для обработки конфиденциальной информации;
передавать документы, содержащие персональные данные, подлежащие защите, по открытым каналам связи (факсимильная связь, электронная почта и т.п.), а также использовать сведения,

содержащие персональные данные, подлежащие защите, в открытой переписке и при ведении переговоров по телефону;
снимать копии с документов, содержащих персональные данные, подлежащие защите, без разрешения начальника отдела кадров и главного врача учреждения;
использовать сведения, содержащие персональные данные, подлежащие защите, в неслужебных целях, в разговоре с лицами, не имеющими отношения к этим сведениям.
5.3. Лица, командированные в учреждение, допускаются к сведениям, содержащим персональные данные работников, решением главного врача в объеме выполнения командировочного задания и с соблюдением требований настоящих Правил.
5.4. Документы, содержащие персональные данные, подлежащие защите, хранятся в металлических постоянно запертых шкафах.

6. Доступ к персональным данным

6.1. Право доступа к персональным данным работников учреждения, имеют только сотрудники, определенные приказом главного врача учреждения.

7. Ответственность за разглашение сведений,
содержащих персональные данные, подлежащие защите,
утрату документов, содержащих такую информацию,
и нарушение порядка работы с ней

7.1. Разглашение сведений, содержащих персональные данные, подлежащие защите, или утрата носителей таких сведений влечет за собой последствия, предусмотренные действующим законодательством.
7.2. Персональную ответственность за разглашение сведений, содержащих персональные данные, подлежащие защите, или утрату носителей таких сведений несет работник учреждения, имеющий доступ к этой информации и допустивший ее разглашение или утрату.
7.3. О фактах утраты работником учреждения носителей сведений, содержащих персональные данные, подлежащие защите, либо разглашения этих сведений ставится в известность его непосредственный руководитель, и главным врачом учреждения назначается комиссия для проведения служебной проверки. По результатам служебной проверки составляется акт. Акты на утраченные дела постоянного хранения передаются в архив.
7.4. Лица, виновные в разглашении или утрате сведений, содержащих персональные данные, подлежащие защите, несут ответственность в соответствии с законодательством Российской Федерации.
7.5. Контроль за исполнением работниками учреждения требований настоящих Правил возлагается на заведующих отделений (руководителей отделов) учреждения.

Экз. № 1

УТВЕРЖДАЮ
Главный врач
МБУЗ «Городская больница №1»

_____ Трусов А.С.

«___» _____ 20__ года
м.п.

АКТ№____

ОПРЕДЕЛЕНИЯ НЕОБХОДИМОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Город Новочеркасск 20___ год

Комиссия по персональным данным,

созданная в МБУЗ «Городская больница №1» (далее по тексту – Учреждение) в соответствии с приказом Главного врача МБУЗ «Городская больница №1» № ____ от «___» _____ 20___ года,

в составе:

Председатель комиссии:

ФИО	**Должность**

Члены комиссии:

ФИО	**Должность**

с целью

самостоятельной экспертной оценки необходимого уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных Учреждения,

рассмотрев

результаты по сбору и анализу исходных данных на информационные системы персональных данных (далее по тексту - ИСПДн) Учреждения, представленные в Отчете о результатах проведения внутренней проверки, утвержденном Главным врачом Учреждения «___» _____ 20___ года,

на основании

- того, что в Отчете о результатах проведения внутренней проверки, утвержденном Главным врачом Учреждения «___» _____ 20___ года, была выделена информационная система персональных данных, названная для внутренней идентификации «_____» (ИСПДн №1 «_____»);
- Акта по оценке возможного вреда субъектам, чьи персональные данные обрабатываются в информационной системе персональных данных «_____» от «___» _____ 20__ года, утвержденного Главным врачом Учреждения «___» _____ 20____ года,
- Частной модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Бухгалтерия и кадры», утвержденной Главным врачом учреждения «___» _____ 20__ года,

во исполнение требований

Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее Постановление Правительства №1119),
и пункта 5 части 1 статьи 18^1 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»,

в соответствии с нормой

пункта 7. Постановления Правительства № 1119 о том, что определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом проведенной Обществом оценки возможного вреда,

с учетом методологии

указанной в совместном Приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»

определила:

I.

ИСПДн №1 «_____» является информационной системой, обрабатывающей **_____ категории** персональных данных, так как в ИСПДн №1 не обрабатываются персональные данные, относящиеся к специальной категории ПДн (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн), или к биометрическим персональным данным (ПДн, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн), или к общедоступным персональным данным (ПДн, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»).

II.

ИСПДн №1 «_____» является информационной системой, обрабатывающей персональные данные **в объеме _____**.

III.

В связи с тем, что в ИСПД №1 «_____» используется лицензионное, но не сертифицированное прикладное программное обеспечение, то для ИСПД №1 **актуальны угрозы _____-го типа**, в том числе, актуальны угрозы, связанные с _____

IV.

ИСПДн №1 «_____» является информационной системой, обрабатывающей персональные данные работников Общества и иные категории персональных данных субъектов персональных данных, не являющихся работниками Общества.

V.

ИСПДн №1 «_____», по заданным характеристикам безопасности, относится к **_____ информационным системам,** в которых требуется обеспечение конфиденциальности, доступности и целостности персональных данных.

VI.

По структуре ИСПДн №1 «_____» представляет собой **_____ информационную систему**, состоящую из комплексов автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа.

VII.

ИСПДн №1 «_____» **имеет подключения** к сетям международного информационного обмена.

VIII.

В ИСПДн №1 «_____» установлен **_____** режим обработки персональных данных.

IX.

В ИСПДн №1 «_____» обработка персональных данных осуществляется **с разграничением прав доступа** пользователей.

X.

Весь аппаратный комплекс и рабочие места ИСПДн №1 «_____» находятся в пределах Российской Федерации.

ВЫВОД:

По результатам проведенного анализа, и, исходя из того, что для информационной системы персональных данных «_____» (ИСПДн №1 «_____») актуальны угрозы ____ -го типа, и в ней обрабатываются иные категории персональных данных работников Учреждения и иные категории персональных данных _____ субъектов персональных данных, не являющихся работниками Учреждения, комиссия пришла к заключению, что для ИСПДн №1 «_____» необходимо обеспечить ____ -й уровень защищенности персональных данных при их обработке в информационной системе.

Комиссия устанавливает, что **для обеспечения ___ -го уровня защищенности** персональных данных при их обработке в ИСПДн №1 «_____» необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена ИСПДн №1, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение главным врачом учреждения документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн №1, необходим для выполнения ими трудовых обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

д) Приказом Главного врача учреждения должен быть назначен работник, ответственный за обеспечение безопасности персональных данных, в том числе, и в ИСПДн №1.

Председатель комиссии:

_____ _____ _____

должность подпись Ф.И.О.

Члены комиссии:

_____ _____ _____

должность подпись Ф.И.О.

_____ _____ _____

должность подпись Ф.И.О.

_____ _____ _____

должность подпись Ф.И.О.

_____ _____ _____

должность подпись Ф.И.О.

«___» _____ 20_ года