ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ВОРОНЕЖСКОЙ ОБЛАСТИ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ ВОРОНЕЖСКОЙ ОБЛАСТИ
«РОССОШАНСКАЯ РАЙОННАЯ БОЛЬНИЦА»
(БУЗ ВО «РОССОШАНСКАЯ РБ»)

ПРИКАЗ

24 апреля 2017г. № 141

г.Россошь

О работе по защите персональных данных в БУЗ ВО»Россошанская РБ»

Во исполнение гл. 14 Трудового кодекса РФ, Федерального закона от 27.072006 г. № 152 ФЗ «О персональных данных», других действующих нормативно правовых актов РФ, в целях обеспечения соблюдения трудового законодательства и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества

ПРИКАЗЫВАЮ:

1. Возложить ответственность за организацию работы с персональными данными в БУЗ ВО «Россошанская РБ» заместителя главного врача по медицинскому обслуживанию населения М.А.Кравченко.

2.Создать комиссию по приведению в соответствие с требованиями Федерального закона от 27 июля 2006 года №152-ФЗ "О персональных данных" в составе:

Председатель комиссии:

Заместитель главного врача по медицинскому обслуживанию населения М.А.Кравченко.

Члены комиссии:

Начальник отдела кадров Н.П.Сыроватская

Начальник отдела АСУ А.М.Тихонов

Юрисконсульт А.В.Сакардин

Секретарь комиссии:

Делопроизводитель Д.А.Морозова

3. Возложить на созданную комиссию задачу по классификации информационных систем персональных данных, а также иные задачи по приведению БУЗ ВО «Россошанская РБ» в соответствие с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных".

4. Назначить ответственными за организацию работы по сбору, обработке и хранению персональных данных работников БУЗ ВО «Россошанская РБ» следующих сотрудников:

4.1. начальника отдела кадров Н.П.Сыроватскую – за сбор, обработку и хранение персональных данных работников в отделе кадров РБ;

4.2. главного бухгалтера РБ Т.Н.Каюрову - за сбор, обработку и хранение персональных данных работников в бухгалтерии.

5. Лицам, ответственным за организацию сбора, обработки и хранения персональных данных работников, обеспечить ознакомление всех сотрудников РБ, имеющих допуск к персональным данным работников, с Положением о защите персональных данных работников.

6. Назначить ответственными за организацию работы по сбору, обработке и хранению персональных данных пациентов:

6.1. по стационарным подразделениям – заместителя главного врача по лечебной работе С.В.Всесвятскую;

6.2. по взрослой поликлинике и прикрепленным ФАПам, стоматологической поликлинике – заместителя главного врача по поликлинической работе Г.В.Якшину;

6.3. по детской поликлинике, женской консультации, гинекологическому, акушерскому, детскому отделениям стационара – заместителя главного врача по детству и родовспоможению В.В.Лобову;

6.4. по участковым больницам с.Новая Калитва, с.Кривоносово, врачебным амбулаториям с.Александровка, с.Архиповка, с.Евстратовка, пос.Начало,

с.Подгорное, с.Поповка и прикрепленным ФАПам – заместителя главного врача по медицинскому обслуживанию населения М.А.Кравченко.

7. Лицам, ответственным за организацию работы по сбору, обработке и хранению персональных данных пациентов, обеспечить ознакомление всех сотрудников РБ, имеющих допуск к персональным данным пациентов, с Положением о защите персональных данных пациентов.

8. Назначить ответственным за информационную безопасность в БУЗ ВО «Россошанская РБ» начальника отдела АСУ А.М.Тихонова.

9. Ответственному за информационную безопасность периодически, но не реже одного раза в месяц, осуществлять контроль эффективности защиты информации в ИСПДн.

10. Утвердить:

10.1. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (Приложение №1);

10.2. Положение о защите персональных данных работников БУЗ ВО «Россошанская РБ» (Приложение №2);

10.3. Положение о защите персональных данных пациентов в БУЗ ВО «Россошанская РБ» (Приложение №2);

10.4. Подписной лист к Положению "О защите персональных данных работников" (Приложение №4);

10.5. Подписной лист к Положению "О защите персональных данных пациентов" (Приложение №5);

10.6. Обязательство о неразглашении персональных данных работников (Приложение №6);

10.7. Уведомление об обработке (о намерении осуществлять обработку) персональных данных (Приложение №7);

10.8. Акт об уничтожении персональных данных, содержащихся на бумажных носителях (Приложение №8);

10.9. Перечень лиц, допущенных к сбору, обработке и хранению персональных данных работников (Приложение №9);

10.10. Перечень лиц, допущенных к сбору, обработке и хранение персональных данных пациентов (Приложение №9).

11. Создать комиссию по уничтожению персональных данных работников, содержащихся на бумажных носителях в составе:

Председатель комиссии:

Заместитель главного врача по медицинскому обслуживанию населения М.А.Кравченко.

Члены комиссии:

Начальник отдела кадров Н.П.Сыроватская

Главный бухгалтер Т.Н.Каюрова

Юрисконсульт А.В.Сакардин

Секретарь комиссии:

Специалист по кадрам О.В.Жарая

12. Создать комиссию по уничтожению персональных данных паациентов, содержащихся на бумажных носителях в составе:

Председатель комиссии:

Заместитель главного врача по лечебной работе С.В.Всесвятская

Члены комиссии:

Зам. главного врача по поликлинической работе Г.В.Якшина

Зам. главного врача по детству и родовспоможеню В.В.Лобова

Юрисконсульт А.В.Сакардин

Секретарь комиссии:

И.о. заведующего ОМО Е.В.Саприна

13. Контроль исполнения настоящего приказа оставляю за собой.

Главный врач Г.Н.Дымова

Приложение №1

УТВЕРЖДЕНО
Приказом БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в БУЗ ВО «Россошанская РБ»

1. Настоящее Положение разработано в соответствии со статьёй 19 Федерального закона «О персональных данных» и устанавливает требования к 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 (далее – информационные системы).

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

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

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (крипографические) средства, средства предотвращения несанкционированного доступа, утечки информации по

техническим каналам, программо-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

3. Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оцениваются при проведении государственного контроля и надзора.

4. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

5. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

6. Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных (далее – оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

7. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается

путём реализации соответствующих организационных мер и (или) путём применения технических средств.

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

9. Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

10. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее – уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

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

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

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищённости персональных данных;

12. Мероприятия по обеспечению безопасности персональных данных при их обработке, в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

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

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

е) учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учёт лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплутационной и технической документацией;

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

к) описание системы защиты персональных данных.

13. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.
14. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных

(трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утверждённого оператором или уполномоченным лицом.

15. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 14 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяются соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

16. При обнаружении нарушений порядка предоставления персональных данных операторов или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

17. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, проводятся тематические исследования в целях проверки выполнения требований по безопасности информации. При этом под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под контрольными тематическими исследованиями – периодически проводимые тематические исследования.

Конкретные сроки проведения контрольных тематических исследований определяются Федеральной службой безопасности Российской Федерации.

18. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

19. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных

системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

20. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учёту с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

21. Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

СОГЛАСОВАНО

Главный бухгалтер Т.Н.Каюрова

Начальник отдела кадров Н.П.Сыроватская

Юрисконсульт А.В.Сакардин

Приложение №2

УТВЕРЖДЕНО
Приказом БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

Положение о защите персональных данных работников БУЗ ВО «Россошанская РБ»

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников БУЗ ВО «Россошанская РБ» от несанкционированного доступа, неправомерного их использования или утраты.
1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона "Об информации, информатизации и защите информации".
1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
1.4. Настоящее Положение утверждается и вводится в действие приказом главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.
2.2. В состав персональных данных работника входят:
- анкетные и биографические данные;
- образование;
- 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;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- 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;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

2.3. Документы, указанные в п. 2.2. настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Обработка персональных данных работника 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 работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.

3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.2.4. Персональные данные следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения

персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.
3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.
3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:
- бухгалтерии;
- сотрудники отдела кадров;
- сотрудники отдела АСУ.
3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
3.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.
3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:
- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.
3.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
3.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.
3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.
3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).
4.1.1. Право доступа к персональным данным сотрудника имеют:
- главный врач Россошанской РБ;
- заместители главного врача, руководители структурных подразделений (доступ к личным данным только сотрудников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового

подразделения;
- сам работник, носитель данных;
- другие сотрудники организации при выполнении ими своих служебных обязанностей.
4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом главного врача организации.
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 перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.
4.2.4. Другие организации.
Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.
Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия (УК 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 незаинтересованные 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 компании.
5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральными законами.
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 обеспечении 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 сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу, работникам отдела кадров и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного

подразделения (например, при подготовке материалов для аттестации работника).
5.5.3. Защита персональных данных сотрудника на электронных носителях. Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается начальнику отдела кадров и начальнику отдела АСУ.
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 РБ, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров.
5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:
- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- 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, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.
6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки

персональных данных работников, а также об их правах и обязанностях в этой области.
6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:
- требовать исключения или исправления неверных или неполных персональных данных;
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.
6.4. Работник обязан:
- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.
- своевременно сообщать работодателю об изменении своих персональных данных.
6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.
6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

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

7.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку

и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.
7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.
7.5.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.
7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.
7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Составил:
Заместитель главного врача
по медицинскому обслуживанию населения М.А.Кравченко

Согласовано:
Главный бухгалтер Т.Н.Каюрова

Начальник отдела кадров Н.П.Сыроватская
Юрисконсульт А.В.Сакардин

Приложение №3

УТВЕРЖДЕНО
Приказом БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

Положение о защите персональных данных пациентов в БУЗ ВО «Россошанская РБ»

1. Общие положения

1.1. Целью данного Положения является защита персональных данных пациентов БУЗ ВО «Россошанская РБ» от несанкционированного доступа, неправомерного их использования или утраты.
1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона "Об информации, информатизации и защите информации".
1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.
1.4. Настоящее Положение утверждается и вводится в действие приказом главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным пациентов.

2. Понятие и состав персональных данных

2.1. Персональные данные пациента - информация, необходимая для медицинских работников в процессе осуществления их профессиональной деятельности и касающиеся конкретного пациента. Под информацией о пациентах понимаются сведения о фактах, событиях и обстоятельствах жизни и здоровья пациента, позволяющие идентифицировать его личность.
2.2. В состав персональных данных пациента входят:
- анкетные и биографические данные;
- сведения о трудовой деятельности;
- сведения о родственниках;
- паспортные данные;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- адрес места жительства;
- мобильный и/или домашний телефон;
- амбулаторная карта, обменная карта, истории болезни пациента;

- журналы заседания врачебной комиссии, КИЛИ
2.3. Документы, указанные в п. 2.2. настоящего Положения, являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. Под обработкой персональных данных пациента понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных пациента.
3.2. В целях обеспечения прав и свобод человека и гражданина сотрудники БУЗ ВО «Россошанская РБ» при обработке персональных данных пациента обязаны соблюдать следующие общие требования:
3.2.1. Обработка персональных данных пациента может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, оказания пациенту медицинской помощи и обеспечения сохранности имущества.
3.2.2. При определении объема и содержания обрабатываемых персональных данных пациента сотрудники Россошанской РБ должны руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами.
3.2.3. Получение персональных данных может осуществляться как путем представления их самим пациентом, так и путем получения их из иных источников.
3.2.4. Персональные данные пациента следует получать у него самого. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Медицинский работник должен сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение.
3.2.5. Медицинский работник не имеет права получать и обрабатывать персональные данные пациента о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами личных, данные о частной жизни пациента (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны медицинским работником только с его письменного согласия.
3.2.6. Медицинский работник не имеет право получать и обрабатывать персональные данные пациента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.3. К обработке, передаче и хранению персональных данных пациента могут иметь доступ сотрудники:
- медицинские работники;
- сотрудники отдела по работе со страховыми медицинскими компаниями по осуществлению взаиморасчетов и проведению анализа деятельности организации;
- сотрудники экономического отдела;
- сотрудники отдела АСУ.
3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.
3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
3.5. Передача персональных данных пациента возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.
3.5.1. При передаче персональных данных пациента должны соблюдаться следующие требования:
- не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные пациента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными пациентов в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций;
3.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
3.5.3. При передаче персональных данных пациента потребителям (в том числе и в коммерческих целях) за пределы медицинской организации, не

должен сообщаться эти данные третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента или в случаях, установленных федеральным законом.
3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных пациентов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.
3.9. При принятии решений, затрагивающих интересы пациента, медицинский работник не имеет права основываться на персональных данных пациента, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).
4.1.1. Право доступа к персональным данным пациента имеют:
- сотрудники регистратуры;
- медицинские работники;
- сотрудники отдела по работе со страховыми медицинскими компаниями по осуществлению взаиморасчетов и проведению анализа деятельности организации;
- сотрудники отдела АСУ.
- другие сотрудники организации при выполнении ими своих служебных обязанностей.
4.1.2. Перечень лиц, имеющих доступ к персональным данным пациентов, определяется приказом главного врача РБ.
4.2. Внешний доступ.
4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- медицинские страховые компании;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

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

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 незаинтересованные 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 компании.
5.4. Защита персональных данных пациентов от неправомерного их использования или утраты должна быть обеспечена администрацией РБ за счет его средств в порядке, установленном федеральными законами.
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 работниками организации.
5.5.2. Для обеспечении внутренней защиты персональных данных пациентов 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 сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

5.5.3. Защита персональных данных пациентов на электронных носителях. Все папки, содержащие персональные данные пациентов, должны быть защищены паролем, который сообщается персоналу кабинета (подразделения) и начальнику отдела АСУ.

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 Россошанской РБ, пациенты и их родственники, 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 РБ.

5.6.3. Для обеспечения внешней защиты персональных данных пациентов необходимо соблюдать ряд мер:
- порядок приема пациентов;
- пропускной режим организации;
- учет медицинской документации и порядок выдачи справок, заключений;
- 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.

6. Права и обязанности пациента

6.1. Закрепление прав пациента, регламентирующих защиту его

персональных данных, обеспечивает сохранность полной и точной информации о нем.
6.2. Пациенты и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных пациентов, а также об их правах и обязанностях в этой области.
6.3. В целях защиты персональных данных пациент имеет право:
- требовать исключения или исправления неверных или неполных персональных данных;
- на бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, в соответствии с действующим законодательством;
- определять своих представителей для получения информации о своих персональных данных;
- на сохранение врачебной тайны, защиту своей личной и семейной тайны.
6.4. Пациент обязан:
- передавать медицинским работникам комплекс достоверных, документированных персональных данных, состав которых установлен законодательством РФ.
- своевременно сообщать медицинским работникам об изменении своих персональных данных.
6.5. В целях защиты частной жизни, личной и семейной тайны пациенты не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

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

7.1. Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.
7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную,

административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым кодексом дисциплинарные взыскания.
7.5.2. Работники Россошанской РБ, в обязанность которых входит ведение персональных данных пациентов, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.
7.5.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую врачебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на пациентов.
7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.
7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Составил:
Заместитель главного врача
по медицинскому обслуживанию населения М.А.Кравченко

Согласовано:
Начальник отдела кадров Н.П.Сыроватская

Юрисконсульт А.В.Сакардин

Начальник отдела АСУ А.М.Тихонов

Приложение №4
к приказу БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

Подписной лист
к Положению "О защите персональных данных работников"

С Положением "О защите персональных данных работников" БУЗ ВО «Россошанская РБ» ознакомлен(а).

Фамилия, Имя, Отчество	Должность	Подразделение	Дата ознакомления	Роспись

Приложение №5
к приказу БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

Подписной лист
к Положению "О защите персональных данных пациентов"

С Положением "О защите персональных данных работников" БУЗ ВО «Россошанская РБ» ознакомлен(а).

Фамилия, Имя, Отчество	Должность	Подразделение	Дата ознакомления	Роспись

Приложение №6
к приказу БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

Обязательство
о неразглашении персональных данных работников

Я, _____
(Фамилия Имя Отчество)

_____,
(наименование должности и подразделения)

обязуюсь не разглашать персональные данные работников, ставшие мне известными в связи с исполнением своих должностных обязанностей.

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

Фамилия И.О. _____ _____
(наименование должности работника, который ознакомлен с текстом Положения) (роспись)

"__" _____ 20__ г.

Приложение №7
к приказу БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

Уведомление об обработке (о намерении осуществлять обработку) персональных данных

(полное и сокращенное наименования, фамилия, имя отчество оператора)

(адрес местонахождения и почтовый адрес оператора)

руководствуясь:

(правовое основание обработки персональных данных)

с целью:

(цель обработки персональных данных)

осуществляет обработку:

(категории персональных данных)

принадлежащих:

(категории субъектов, персональные данные которых обрабатываются)

Обработка вышеуказанных персональных данных будет осуществляться путем:

(перечень действий с персональными данными, общее описание используемых оператором способов

обработки персональных данных)

Для обеспечения безопасности персональных данных принимаются следующие меры:

(описание мер, предусмотренных ст.ст.18.1. и 19 Федерального закона N 152-ФЗ от 27.07.2006 "О персональных данных"

в т.ч. сведения о наличии шифровальных (криптографических)

средств и наименования этих средств; фамилия, имя, отчество физического лица или наименование

юридического лица, ответственных за организацию обработки персональных данных,

и номера их контактных телефонов, почтовые адреса и адреса электронной почты)

Сведения о наличии или об отсутствии трансграничной передачи персональных данных:

(при наличии трансграничной передачи персональных данных в процессе их обработки, указывается

перечень иностранных государств, на территорию которых осуществляется трансграничная передача

персональных данных)

Сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации:

(страна, адрес местонахождения базы данных,

наименование информационной системы (базы данных)

Сведения об обеспечении безопасности персональных данных:

(сведения об обеспечении безопасности персональных данных в соответствии с требованиями

к защите персональных данных, установленными Правительством Российской Федерации)

Дата начала обработки персональных данных _____
(число, месяц, год)

Срок или условие прекращение обработки персональных данных:

(число, месяц, год или основание (условие), наступление которого повлечет прекращение обработки

персональных данных)

_____ _____ _____
(должность) (подпись) расшифровка подписи

"___"_____20___г.

Приложение №8
к приказу БУЗ ВО
«Россошанская РБ»
от 24.04.2017г. №141

БУЗ ВО «Россошанская РБ»

Акт об уничтожении персональных данных, содержащихся на бумажных носителях

г.Россошь "__" __ 20__ г.

Комиссия, наделенная полномочиями приказом БУЗ ВО «Россошанская РБ» от 24.04.2017г. №141, в составе __ (__) человек:

Председатель комиссии: (должность, Ф.И.О.) .

Члены комиссии: (должность, Ф.И.О.) .

составила настоящий акт о том, что "__" __ 20__ г. в полном соответствии с положениями Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" ей было произведено уничтожение персональных данных (категория лиц, чьи персональные данные были уничтожены) , находящихся на нижеуказанных бумажных носителях, хранящихся в (наименование организации) , тип информации - __:

N п/п	Учетный/иной номер носителя	Наименования носителя	Пояснения

Уничтожение информации произведено путем (механического уничтожения (разрезания/измельчения), сжигания и т.п.) , гарантирующим полное уничтожение персональных данных.

Основание для производства уничтожения персональных данных: (выявление неправомерных действий с персональными данными, достижение цели обработки персональных данных, отзыв субъектом персональных данных согласия на обработку своих персональных данных, иное основание) .

Председатель комиссии _____/_____

Члены комиссии _____/_____

_____/_____

СОГЛАСОВАНИЕ

проекта приказа БУЗ ВО «Россошанская РБ»: «**О работе по защите персональных данных в БУЗ ВО»Россошанская РБ»**

Должность	Инициалы, фамилия	Дата согласования	Замечания	Подпись
Заместитель главного врача по медицинскому обслуживанию населения	М.А.Кравченко			
Начальник отдела кадров	Н.П.Сыроватская			
Юрисконсульт	А.В.Сакардин			

Приказ разослать:

Кравченко Марина Анатольевна	Лобов Николай Иванович
Якшина Галина Валерьевна	Фролова Екатерина Дмитриевна
Всесвятская Светлана Викторовна	Лозовиков Евгений Анатольевич
Лобова Вера Владимировна	Фролов Алексей Владимирович
Чичмарева Екатерина Евгеньевна	Березкина Галина Юрьевна
Ярошева Наталья Дмитриевна	Цыбин Виктор Александрович
Ловцов Виктор Иванович	Романцова Ирина Александровна
Каюрова Таисия Николаевна	Нестерова Ирина Юрьевна
Сыроватская Наталья Петровна	Есин Александр Александрович
Сакардин Александр Владимирович	Левин Алексей Валентинович
Анисимова Полина Денисовна	Гузиков Евгений Викторович
Копаев Олег Владимирович	Странковский Павел Владимирович
Ковалев Сергей Андреевич	Глущенко Сергей Тихонович
Нестеров Алексей Николаевич	Коновалова Анна Александровна
Чичмарев Николай Васильевич	Бондарь Валентина Петровна
Шаповалова Ольга Петровна	Чужинова Светлана Леонидовна
Лозенко Вера Александровна	Кривошеева Алина Александровна
Кузнецова Татьяна Ивановна	Зинченко Игорь Владимирович
Коровкова Надежда Анатольевна	Кузичкин Николай Федорович
Кондакова Светлана Владимировна	Лозовая Галина Николаевна
Саприна Елена Владимировна	Ярошева Елена Валерьевна
Тихонов Андрей Михайлович	Власенко Светлана Николаевна
Заиченко Сергей Станиславович	Кузнецов Виктор Федорович
Жарая Оксана Валериевна	Звягинцева Ирина Леонидовна
	Морозова Дарья Александровна

Исполнитель, телефон М.А.Кравченко (47396)2-52-56
(подпись)

Передано в дело_____экз____._____. 2017 года
Секретарь _____ Н.Н.Лахина

Лист ознакомления с приказом БУЗ ВО «Россошанская РБ»
от «24 » апреля 2017 года № 141
«**О работе по защите персональных данных в БУЗ ВО»Россошанская РБ»**

№ п/п	Фамилия, имя отчество	Должность	Подпись	Дата
1.	Кравченко Марина Анатольевна	Зам. главного врача по медицинскому обслуживанию населения		
2.	Якшина Галина Валерьевна	Зам. главного врача по поликлинической работе		
3.	Всесвятская Светлана Викторовна	Зам. главного врача по лечебной работе		
4.	Лобова Вера Владимировна	Зам. главного врача по детству и родовспоможению		
5.	Чичмарева Екатерина Евгеньевна	Зам. главного врача по КЭР		
6.	Ярошева Наталья Дмитриевна	Зам. главного врача по экономическим вопросам		
7.	Ловцов Виктор Иванович	Заведующий стоматологической поликлиникой		
8.	Каюрова Таисия Николаевна	Главный бухгалтер РБ		
9.	Сыроватская Наталья Петровна	Начальник отдела кадров РБ		
10	Сакардин Александр Владимирович	Юрисконсульт РБ		
11	Анисимова Полина Денисовна	Главная медицинская сестра РБ		
12	Копаев Олег Владимирович	Заведующий хирургическим отделением		
13	Ковалев Сергей Андреевич	Заведующий травматологическим отделением		
14	Нестеров Алексей Николаевич	Заведующий урологическим отделением		
15	Чичмарев Николай Васильевич	Заведующий АРО		
16	Шаповалова Ольга Петровна	Заведующая гинекологическим отделением		
17	Лобов Николай Иванович	Заведующий инфекционным отделением		
18	Фролова Екатерина Дмитриевна	Заведующая детским отделением		
19	Лозовиков Евгений Анатольевич	Заведующий акушерским отделением		
20	Фролов Алексей Владимирович	Заведующий женской консультацией		
21	Березкина Галина Юрьевна	Заведующая психиатрическим отделением		

22	Цыбин Виктор Александрович	Заведующий наркологическим отделением		
23	Романцова Ирина Александровна	Заведующая кардиологическим отделением		
24	Нестерова Ирина Юрьевна	Заведующая терапевтическим отделением		
25	Есин Александр Александрович	Заведующий неврологическим отделением		
26	Левин Алексей Валентинович	Заведующий отделением скорой медицинской помощи		
27	Гузиков Евгений Викторович	Заведующий УБ с.Новая Калитва		
28	Странковский Павел Владимирович	Заведующий УБ с.Кривоносово		
29	Глущенко Сергей Тихонович	Врач общей практики ВА с.Александровка		
30	Коновалова Анна Александровна	Врач общей практики ВА с.Архиповка		
31	Бондарь Валентина Петровна	Врач общей практики ВА с.Евстратовка		
32	Чужинова Светлана Леонидовна	Врач общей практики ВА с.Поповка		
33	Кривошеева Алина Александровна	Врач-терапевт участковый ВА пос.Начало		
34	Зинченко Игорь Владимирович	Врач-терапевт участковый ВА с.Подгорное		
35	Кузичкин Николай Федорович	Заведующий отделением ВОП поликлиники		
36	Лозовая Галина Николаевна	Заведующая отделением ВОП поликлиники		
37	Ярошева Елена Валерьевна	Заведующая отделением платных услуг		
38	Власенко Светлана Николаевна	Заведующая клинико-диагностической лабораторией		
39	Кузнецов Виктор Федорович	Заведующий рентгенологическим отделением		
40	Звягинцева Ирина Леонидовна	Заведующая физиоте-рапевтическим отделением		
41	Заиченко Сергей Станиславович	Врач-эпидемиолог		
42	Лозенко Вера Александровна	Зав. отделением медицинской профилактики		
43	Кузнецова Татьяна Ивановна	И.о. зав. диагностическим отделением		
44	Коровкова Надежда Анатольевна	Зав. детской поликлиникой		
45	Кондакова Светлана Владимировна	Заведующая педиатрическим отделением детской поликлиники		
46	Саприна Елена Владимировна	И.о. зав. организационно-методическим отделением		
47	Тихонов Андрей	Начальник отдела АСУ		

	Михайлович			
48	Жарая Оксана Валериевна	Специалист по кадрам		
49	Морозова Дарья Александровна	Делопроизводитель		