ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «СПЕЦИАЛИЗИРОВАННАЯ ПСИХИАТРИЧЕСКАЯ БОЛЬНИЦА № 3» МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ КРАСНОДАРСКОГО КРАЯ

ПРИКАЗ

от 09.01.2018 г. **№ 152- п**

Об утверждении политики в сфере сбора, обработки и защиты персональных данных в ГБУЗ СПБ №3

Во исполнение требований Федерального закона Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», Постановления правительства Российской Федерации от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» в целях установления методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в ГБУЗ СПБ №3, п р и к а з ы в а ю:

1.Утвердить пакет типовых документов по защите персональных данных работников, пациентов и посетителей государственного бюджетного учреждения здравоохранения «Специализированная психиатрическая больница №3» министерства здравоохранения Краснодарского края (ГБУЗ СПБ № 3) согласно приложений (с № 1 по № 15).

2. Должностным лицом, ответственным за обработку персональных данных, осуществляемой без использования средств автоматизации назначить начальника отдела по кадрам Шеходько Л.В.

3. Должностным лицом, ответственным за обработку персональных данных, осуществляемой при их обработке в информационных системах персональных данных назначить ведущего инженера Верченко В.В.

4. Приказ по учреждению от 30.05.2017 года №279-п «Об установлении методов и способов защиты информации, необходимых для обеспечения безопасности персональных данных в ГБУЗ СПБ № 3» считать утратившим силу.

5. Ознакомить с приказом сотрудников учреждения.

6. Контроль исполнения приказа возложить на начальника отдела по кадрам Шеходько Л.В.

7. Приказ вступает в силу со дня его подписания.

Главный врач Л.Н.Борисенко

Проект приказа подготовил:
Юрисконсульт (ведущий) Е.В. Скирева

Согласовано:
заместитель главного врача
по медицинской части А.В. Стаднюк

ведущий инженер В.В. Верченко

начальник отдела по кадрам Л.В. Шеходько

Приложение 1 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

ПОЛОЖЕНИЕ
о политике Государственного бюджетного учреждения здравоохранения «Специализированная психиатрическая больница №3» министерства здравоохранения Краснодарского края (ГБУЗ СПБ №3) в сфере сбора, обработки и защиты персональных данных работников, пациентов, посетителей

1. Общие положения.

1.1. Настоящим Положением определяется порядок получения, учета, обработки, накопления, хранения, передачи и любого другого использования сведений, относящихся к персональным данным работников, пациентов, посетителей ГБУЗ СПБ №3.

1.2. Цель настоящего Положения обеспечить защиту пациентов, работников, посетителей больницы от несанкционированного доступа к их персональным данным и их разглашения, обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.2004г. №98-ФЗ «О коммерческой тайне», Федеральным законом от 22.10.2004г. №125-ФЗ «Об архивном деле в Российской Федерации», Указом Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера» и другими действующими нормативными актами РФ.

1.4. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями больницы.

1.5. Руководители структурных подразделений и ответственные за работу с персональными данными должны быть ознакомлены под роспись с настоящим Положением, со всеми дополнениями и изменениями к нему и довести их до сотрудников подразделения и пациентов.

2. Основные понятия, используемые в настоящем положении.

2.1. В целях настоящего Положения используются следующие основные понятия, термины и сокращения:

1) **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) **персональные данные работника** – это информация, необходимая больнице в связи с трудовыми отношениями и касающаяся конкретного работника.

3) **персональные данные пациента** – это информация, необходимая больнице для обеспечения организации лечебного процесса и касающаяся конкретного пациента.

4) оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными; **далее по тексту приказа под Оператором подразумевается ГБУЗ СПБ №3**;

5) **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или

без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

6) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

7) **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

8) **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

9) **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

10) **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;

11) **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

12) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

13) **конфиденциальность персональных данных** – обязательное для соблюдения больницей или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия работника (пациента) или наличия иного законного основания.

14) автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

15) аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному;

16) безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

17) биометрические персональные данные - сведения, которые характеризуют физиологические особенности человека, и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию;

18) вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения;

19) вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на персональные данные или ресурсы информационной системы персональных данных;

20) вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных;

21) доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ;

22) доступ к информации - возможность получения информации и ее использования;

23) закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

24) защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

25) идентификация - присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

26) информативный сигнал - электрический сигнал, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных;

26) информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

27) информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

28) использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

29) источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;

30) контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств;

31) межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и/или выходящей из информационной системы;

32) нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных;

33) недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации;

34) несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных;

35) носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин;

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

37) перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов;

38) побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания;

39) политика "чистого стола" - комплекс организационных мероприятий, контролирующих отсутствие записи ключей и атрибутов доступа (паролей) на бумажные носители и хранения их вблизи объектов доступа;

40) пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

41) правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

42) программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и/или блокировать аппаратные средства;

43) программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ;

44) раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных;

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

46) ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы;

47) средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

48) субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа;

49) технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети,

средства и системы передачи, приема и обработки ПДн (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;

50) технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;

51) угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных;

52) утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

53) уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации;

54) целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2.2. Перечень персональных данных работников представлен в приложении №1, перечень персональных данных пациентов – в приложении №2, перечень персональных данных посетителей – в приложении №3.

3. Принципы и условия обработки персональных данных

3.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

3.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

3.6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. Условия сбора и обработки персональных данных.

4.1. обработка персональных данных осуществляется с согласия работника (пациента) персональных данных на обработку его персональных данных;

4.2. обработка персональных данных необходима для достижения целей, предусмотренных для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей; обработка персональных данных работника (пациента) может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам (пациентам) в трудоустройстве, лечении и продвижении по службе, обеспечения личной безопасности, контроля прохождения лечения, количества и качества выполняемой работы и обеспечения сохранности имущества.

4.3. При определении объема и содержания обрабатываемых персональных данных оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ, Федеральным законом от 27.07.2006г. №152-ФЗ «О персональных данных» и иными федеральными законами.

4.4. Все персональные данные работника (пациента) следует получать у него самого. Обработка персональных данных работника (пациента) осуществляется только с его согласия в установленной письменной форме

4.5. Обработка и использование персональных данных осуществляется в целях, указанных в письменном согласии работника (пациента) на обработку его персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами РФ.

4.6. Если персональные данные работника (пациента) возможно получить только у третьей стороны, то работник (пациент) должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

4.7. В случае недееспособности работника (пациента) согласие на обработку его персональных данных дает в письменной форме законный представитель работника (пациента).

4.8. Если персональные данные были получены не от работника (пациента), за исключением случаев, если персональные данные были предоставлены больнице на основании федерального закона или если персональные данные являются общедоступными, больница до начала обработки таких персональных данных обязана предоставить работнику (пациенту) следующую информацию:

- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные действующим законодательством РФ права работника (пациента).

4.9. В случае смерти работника (пациента) согласие на обработку его персональных данных дают в письменной форме его наследники, если такое согласие не было дано работником (пациентом) при его жизни.

4.10. Больница должна сообщить работнику (пациенту) о последствиях отказа дать письменное согласие на их получение.

4.11. Согласия работника (пациента) на обработку его персональных данных не требуется в следующих случаях:

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является работник (пациент);
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника (пациента), если получение его согласия невозможно;
- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи

расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

- обработка персональных данных осуществляется в целях научной, литературной или иной творческой деятельности работника (пациента) при условии, что при этом не нарушаются его права и свободы;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности;
- в иных случаях, предусмотренных законодательством РФ.
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.12. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных.

4.13. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

4.14. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

4.15. Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

4.16. Работник (пациент) принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано работником (пациентом) или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя пациента полномочия данного представителя на дачу согласия от имени пациента проверяются оператором.

4.17. Согласие на обработку персональных данных может быть отозвано работником (пациентом). В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без

согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6**,** части 2 статьи 10 и части 2 статьи 11 Федерального закона №152-ФЗ.

4.18. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме работника (пациента). Равнозначным содержащему собственноручную подпись работника (пациента) согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме работника (пациента) на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес работника (пациента), номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя пациента, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя пациента);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие работника (пациента);

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие работника (пациента), а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись работника (пациента).

4.19. В случае недееспособности пациента согласие на обработку его персональных данных дает законный представитель пациента.

4.20. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

4.21. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6**,** части 2 статьи 10 и части 2 статьи 11 Федерального закона №152-ФЗ.

4.22. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев:

4.22.1. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

4.22.2. обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и

обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

4.22.3. обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

4.22.4. обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исполнительным законодательством Российской Федерации;

4.22.5. обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора;

4.22.6. обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

4.22.7. обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о гражданстве Российской Федерации.

4.23. Обработка специальных категорий персональных данных, незамедлительно прекращается, если устранены причины, вследствие которых осуществлялась обработка, если иное не установлено федеральным законом.

4.24. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности пациента, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 ст.11 152-ФЗ.

4.25. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

4.26. Согласие, подписанное работником (пациентом), действует со дня его подписания до дня отзыва в письменной форме или по истечению 75 лет (работником) или 50 лет (пациентом) с момента подписания.

4.27. В случае увольнения (выписки) работника (пациента) и достижения целей обработки персональных данных, зафиксированных в Письменном соглашении, больница обязана незамедлительно прекратить обработку персональных данных.

4.28. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных могут включаться фамилия, имя, отчество, должность, подразделение, служебные телефоны и адрес электронной почты. Другие персональные данные (например дата рождения и т.д.) могут включаться в справочники только с письменного согласия работника (пациента).

4.29. При принятии решений, затрагивающих интересы работника (пациента), работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5. Права субъекта персональных данных (работника/пациента)

5.1. Работник (пациент) вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.2. Сведения, указанные в пункте 5.7. настоящего положения должны быть предоставлены работнику (пациенту) оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

5.3. Сведения, указанные в пункте 5.7. настоящего положения, предоставляются работнику (пациенту) или его представителю оператором при обращении либо при получении запроса работника (пациента) или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность работника (пациента) или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие работника (пациента) данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись работника (пациента) или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5.4. В случае, если сведения, указанные в пункте 5.7. настоящего положения, а также обрабатываемые персональные данные были предоставлены для ознакомления работнику (пациенту) по его запросу, работник (пациент) вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 5.7. настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является работник (пациент).

5.5. Работник (пациент) вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 4.7. настоящего положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п 4.4. настоящего положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п 4.3. настоящего положения, должен содержать обоснование направления повторного запроса.

5.6. Оператор вправе отказать работнику (пациенту) в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 4.4. и 4.5. настоящего положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

5.7. Работник (пациент) имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут

быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

5.8. Право работника (пациента) на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:
1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
2) обработка персональных данных осуществляется органами, осуществившими работника (пациента) по подозрению в совершении преступления, либо предъявившими работнику (пациенту) обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
4) доступ работника (пациента) к его персональным данным нарушает права и законные интересы третьих лиц;
5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

5.9. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных п.4.10. настоящего положения.

5.10. Решение, порождающее юридические последствия в отношении работника (пациента) или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

5.11. Оператор обязан разъяснить работнику (пациенту) порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и

возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты работником (пациентом) своих прав и законных интересов.

5.12. Оператор обязан рассмотреть возражение, указанное в п.3.11. настоящего положения, в течение тридцати дней со дня его получения и уведомить работника (пациента) о результатах рассмотрения такого возражения.

5.13. Если работник (пациент) считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, работник (пациент) вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

6. Обязанности оператора при сборе персональных данных

6.1. При сборе персональных данных оператор обязан предоставить работнику (пациенту) по его просьбе информацию, предусмотренную п.4.7. настоящего положения.

6.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор разъясняет работнику (пациенту) юридические последствия отказа предоставить его персональные данные.

6.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных п.5.4. настоящего положения, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
2) цель обработки персональных данных и ее правовое основание;
3) предполагаемые пользователи персональных данных;
4) установленные настоящим Федеральным законом права субъекта персональных данных;
5) источник получения персональных данных.

6.4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п.5.3. настоящего положения, в случаях, если:

1) работник (пациент) уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является работник (пациент);
3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной, научной, иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
5) предоставление субъекту персональных данных сведений, предусмотренных 5.3. настоящего положения, нарушает права и законные интересы третьих лиц.

6.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2**,** 3**,** 4**,** 8 части 1 статьи 6 Федерального закона 152-ФЗ.

7. Хранение, обработка и защита персональных данных.

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

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

7.3. Сотрудники ГБУЗ СПБ №3, осуществляющие обработку персональных данных без использования средств автоматизации или лица, осуществляющие такую обработку по договору с оператором, информируются о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а так же об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, настоящим положением.

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

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес ГБУЗ СПБ №3, фамилию, имя, отчество и адрес работника (пациента), источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором работник (пациент) может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

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

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

7.5. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию (посетителей), на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена приказом ГБУЗ СПБ №3, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных (посетителей), перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных (посетителей) на территорию ГБУЗ СПБ№3, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных (посетителем);

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных (посетителя) могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных (посетителя) на территорию ГБУЗ СПБ №3.

7.6. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, в ГБУЗ СПБ №3 принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.7. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7.8. Правила, предусмотренные пунктами 6.6. и 6.7. настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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

7.10. Обработка персональных данных, осуществляемая без использования средств автоматизации, в ГБУЗ СПБ №3 осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

7.11. В ГБУЗ СПБ №3 обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7.12. При хранении материальных носителей в ГБУЗ СПБ №3 соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом по учреждению.

7.13. Персональные данные работников могут храниться в бумажном и (или) электронном виде в отделе кадров, планово-экономическом отделе, бухгалтерии с соблюдением предусмотренных нормативно-правовых актов РФ и мер по защите персональных данных.

7.14. Руководители подразделений, в которых происходит обработка персональных данных, должны обеспечить защиту и конфиденциальность персональных данных, обрабатываемых в их подразделениях.

7.15. Сотрудники больницы, имеющие доступ к персональным данным, обязаны принимать и соблюдать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, распространения, а также от иных неправомерных действий в отношении данной информации.

7.16. Доступ к персональным данным работников имеют в рамках своих должностных обязанностей:

- главный врач
- заместитель главного врача по медицинской части
- начальник отдела кадров
- заместитель главного врача по экономическим вопросам
- главный бухгалтер
- заместитель главного бухгалтера
- начальник отдела (доступ к персональным данным только работников данного отдела)
- руководители структурных подразделений (доступ к персональным данным только работников соответствующего подразделения)
- сотрудники отдела кадров, бухгалтерии, экономического отдела, инженера по охране труда, инженера по пожарной безопасности, юрисконсульта (только к тем персональным данным, которые необходимы для выполнения конкретных функций этих сотрудников)
- сам работник (только к своим персональным данным)

7.17. Доступ к персональным данным пациента в рамках своих должностных обязанностей имеют:

- главный врач
- заместитель главного врача по медицинской части
- главная медицинская сестра
- заведующий отделением (доступ к персональным данным только пациентов соответствующего отделения)
- врач-психиатр (доступ к персональным данным только пациентов, находящихся у него на лечении)
- врачи-консультанты (доступ только к тем персональным данным, которые необходимы для выполнения конкретных функций)
- юрисконсульт (ведущий)
- средний медицинский персонал отделения (доступ к персональным данным только пациентов соответствующего отделения)
- социальный работник
- медицинский статистик
- медицинский регистратор
- сам пациент (только к своим персональным данным)

7.18. Доступ к персональным данным посетителей в рамках своих должностных обязанностей имеют:

- главный врач
- заместитель главного врача по хозяйственным вопросам
- сотрудники охраны учреждения
- юрисконсульт (ведущий)

7.19. Иные сотрудники больницы могут иметь доступ к персональным данным работников (пациентов) в соответствии с изданными приказами или иными утвержденными руководством больницы разрешительными документами.

7.20. Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается.

7.21. К числу массовых потребителей персональных данных работников, (пациентов) вне больницы можно отнести государственные и негосударственные структуры, в том числе:

- правоохранительные органы
- органы прокуратуры, ФСБ, Росгвардии
- налоговые инспекции
- органы лицензирования и сертификации
- страховые агентства
- военкоматы
- органы статистики
- органы социального страхования
- пенсионные фонды
- подразделения муниципальных органов управления

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

7.23. Все документы на бумажных носителях, содержащие персональные данные работников (пациентов) должны храниться в местах, защищенных от несанкционированного доступа.

8. Защита персональных данных при их обработке в информационных системах персональных данных

8.1. Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся состояния здоровья, интимной жизни субъектов персональных данных.

8.2. Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

8.3. Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

8.4. Для ГБУЗ СПБ №3 актуальны угрозы безопасности персональных данных являются угрозы 3-го типа (угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

8.5. Для ГБУЗ СПБ № 3 применяются нормы пп. в) п.11 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 1 ноября 2012 года №1119 – устанавливается необходимость обеспечения 3-го уровня защищенности персональных данных.

8.6. В целях обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах в ГБУЗ СПБ № 3 обеспечивается выполнение следующих требований:

1) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

2) обеспечение сохранности носителей персональных данных;

3) утверждение перечня лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

4) 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;

5) назначение должностного лица, ответственного за обеспечение безопасности персональных данных в информационной системе.

8.7. Доступ к электронным носителям, содержащим персональные данные работников (пациентов) обеспечиваются разграничением прав доступа в информационной системе, а также многоступенчатой системой паролей.

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

8.9. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

8.10. Размещение информационных систем, специальное оборудование и охрана помещений (с помощью систем сигнализации), в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения в эти помещения посторонних лиц.

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

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

8.12. При обнаружении нарушений порядка обработки персональных данных главный врач больницы или заместитель главного врача по медицинской части, начальник отдела по кадрам незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

8.13. Обеспечение технического обслуживания сервера, на котором хранятся персональные данные, возлагается на ведущего инженера-программиста.

8.14. Контроль за выполнением настоящих требований организуется и проводится ГБУЗ СПБ №3 самостоятельно. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые ГБУЗ СПБ №3.

9. Передача персональных данных.

9.1. Сотрудники больницы, ответственные за работу с персональными данными, должны четко знать случаи, при которых они могут передать информацию о работнике (пациенте) запрашивающим лицам. К таким случаям, как правило, относят запросы о получении информации о работниках и пациентах больницы, направленные различными государственными органами.

9.2. Не допускается сообщать третьей стороне персональные данные работника (пациента) без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника (пациента), а также в случаях, установленных законодательством РФ.

9.3. Не допускается сообщать персональные данные работника (пациента) в коммерческих целях без его письменного согласия.

9.4. В случае если лицо, обратившееся с запросом, не уполномочено действующим законодательством РФ на получение персональных данных работника (пациента) либо отсутствует письменное согласие работника (пациента) на предоставление его персональных данных, больница обязана отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных с указанием причины отказа.

9.5. В больнице и во всех ее структурных подразделениях, в которых обрабатываются персональные данные работников (пациентов) необходимо вести журнал учета выданных персональных данных работников (пациентов). В этом журнале регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе предоставления персональных данных, а также указывается список переданных персональных данных.

9.6. При передаче персональных данных работников (пациентов) третьим лицам необходимо предупреждать их 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 (пациента), обязаны соблюдать режим конфиденциальности. Исключение составляет обмен персональными данными в порядке, установленном действующим законодательством.

9.7. Передача персональных данных работников (пациентов) в пределах больницы осуществляется в соответствии с локальными нормативными актами больницы (должностные инструкции сотрудников, имеющих отношение к обработке персональных данных; инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные и другие), положениями о структурных подразделениях, приказами, распоряжениями главного врача больницы.

9.8. Не допускается запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

10. Обязанности оператора (ГБУЗ СПБ № 3)

10.1. ГБУЗ СПБ № 3 обязано:

- осуществлять защиту персональных данных работника (пациента), посетителя, применяя все необходимые организационные и технические меры;
- обеспечить хранение первичной учетной документации по учету труда и его оплаты;

- обеспечить надлежащее хранение первичной медицинской документации.

10.2. ГБУЗ СПБ № 3 обязано безвозмездно предоставить работнику (пациенту) или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему работнику (пациенту).

10.3. ГБУЗ СПБ № 3 обязано сообщить в порядке, предусмотренном статьей 14 Федерального закона №152-ФЗ, работнику (пациенту) или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

10.4. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя ГБУЗ СПБ №3 обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона №152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

10.5. ГБУЗ СПБ № 3 обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, ГБУЗ СПБ № 3 обязано внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. ГБУЗ СПБ №3 обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

10.6. ГБУЗ СПБ № 3 обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

10.7. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных ГБУЗ СПБ №3 обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных ГБУЗ СПБ № 3 обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных дан-

ных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

10.8. В случае подтверждения факта неточности персональных данных ГБУЗ СПБ № 3 на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ГБУЗ СПБ №3) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

10.9. В случае выявления неправомерной обработки персональных данных, осуществляемой ГБУЗ СПБ № 3 или лицом, действующим по поручению ГБУЗ СПБ №3, ГБУЗ СПБ № 3 в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, ГБУЗ СПБ № 3 в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных ГБУЗ СПБ № 3 обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

10.10. В случае достижения цели обработки персональных данных ГБУЗ СПБ № 3 обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ГБУЗ СПБ №3) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ГБУЗ СПБ № 3) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между ГБУЗ СПБ № 3 и субъектом персональных данных либо если ГБУЗ СПБ №3 не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

10.11. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных ГБУЗ СПБ №3 обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению ГБУЗ СПБ № 3) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению ГБУЗ СПБ № 3) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между ГБУЗ СПБ №3 и субъектом персональных данных либо если ГБУЗ СПБ №3 не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

10.12. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в Федеральном законе №152-ФЗ, ГБУЗ СПБ № 3 осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обра-

ботка персональных данных осуществляется другим лицом, действующим по поручению ГБУЗ СПБ № 3) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

11. Обязанности и права работников (пациентов).

11.1. Работник (пациент) обязан:

- передавать больнице комплекс достоверных документированных персональных данных, перечень которых установлен Трудовым кодексом РФ и правилами приема в больницу;
- своевременно в срок, не превышающий одного месяца, сообщать больнице об изменении своих персональных данных.

11.2. Работник (пациент) имеет право:

- на получение сведений о больнице, о месте ее нахождения, о медицинских работниках, сведения о которых размещены на официальном сайте ГБУЗ СПБ № 3, о наличии у больницы персональных данных, относящихся к соответствующему работнику (пациенту), а также на ознакомление с такими персональными данными и получения копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных законодательством РФ;
- требовать от больницы уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных;
- на получение полной информации об обработке своих персональных данных;
- на обжалование действий или бездействия больницы в уполномоченный орган по защите 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.

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

12.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работников (пациентов), установленных действующим законодательством, Положением о порядке работы с конфиденциальной информацией и данным Положением, несут дисциплинарную, административную, гражданскую, уголовную или иную ответственность в соответствии с действующим законодательством РФ.

12.2. Руководители подразделений, в которых происходит обработка персональных данных, несут персональную ответственность за обеспечение защиты обрабатываемых и хранящихся в их подразделениях персональных данных работников (пациентов), посетителей.

Юрисконсульт (ведущий) Е.В. Скирева

Приложение 2 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Перечень персональных данных работников

Фамилия, имя, отчество
Информация о смене фамилии, имени, отчества
Пол
Год, месяц и дата рождения
Место рождения
Гражданство
Реквизиты документа, удостоверяющего личность (серия, номер, кем и когда выдан)
Реквизиты заграничного паспорта
Реквизиты водительского удостоверения (для водителей)
Место и дата регистрации
Место жительства
Номера телефонов (городской, мобильный)
Адрес электронной почты
Семейное положение
Состав семьи
Отношение к воинской обязанности
Воинское звание, состав рода войск
Реквизиты военного билета, приписного свидетельства
Сведения о наличии детей, их возрасте, месте работы (учебы)
Сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах
Сведения о полученном профессиональном и дополнительном образовании (наименование образовательного учреждения, специальность и квалификация по документу об образовании; реквизиты документа об образовании, о квалификации, наличии специальных знаний; наименование документа об образовании, его серия и номер; послевузовское профессиональное образование)
Сведения об уровне профессиональных знаний, о владении специальными умениями и навыками (работа на компьютере, владение иностранными языками и др.)
Ученая степень (отрасль науки, диплом, диссертационный совет, дата присуждения ученой степени)
Ученое звание (аттестат, его номер, дата присвоения ученого звания, научная специальность)
Повышение квалификации
Профессиональная переподготовка
Сведения о предыдущей трудовой деятельности
Трудовая книжка и сведения, содержащиеся в ней (сведения о продолжительности общего трудового стажа, страхового стажа, непрерывного стажа и др.)
Сведения о состоянии здоровья и его соответствии выполняемой работе
Сведения по отпускам и командировкам
Общий медицинский стаж
Наличие научных трудов, изобретений, список научных трудов
Аттестации
Сведения о наградах (поощрениях), взысканиях
Сведения о почетные званиях

ИНН
Номер страхового свидетельства ОПС (ГПС)
Номер страхового полиса (ОМС)
Профессия
Должность
Размер оклада в соответствии с профессиональными группами и уровнями
Заработная плата, включая все выплаты
Наличие и группа инвалидности и степени ограничения способности к трудовой деятельности
Наличие судимостей
Сведения о социальных льготах

Приложение 3 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Перечень персональных данных пациентов.

Фамилия, имя, отчество
Пол
Год, месяц и дата рождения
Место рождения
Документ, удостоверяющий личность (серия, номер, кем и когда выдан)
Место и дата регистрации
Место жительства
Номера телефонов (городской, мобильный)
Номер страхового полиса (ОМС)
Данные медицинской карты
Диагноз
Сведения об анамнезе, обследовании, лечении

Приложение 4 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Перечень персональных данных посетителей.

Фамилия, имя, отчество
Реквизиты (серия и номер) документа, удостоверяющего личность

Приложение 5 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Список подразделений
обрабатывающих персональные данные

1. Приемное отделение
2. Отделение №1
3. Отделение №2
4. Отделение №3
5. Отделение №5
6. Отдел кадров
7. Бухгалтерия
8. Экономический отдел
9. Инженерный отдел
10. Отдел статистики
11. Архив
12. Юрисконсульт

Приложение 6 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

_____
(ДОЛЖНОСТЬ)
_____
(ПОДРАЗДЕЛЕНИЕ)

СОГЛАСИЕ РАБОТНИКА НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
(фамилия, имя, отчество)
проживающий (ая) по адресу
_____
_____
_____

паспорт _____
(серия и номер основного документа, удостоверяющего личность
_____
кем и когда выдан, номер подразделения)

даю свое согласие на обработку с учетом требований действующего законодательства Государственному бюджетному учреждению здравоохранения «Специализированная психиатрическая больница №3» министерства здравоохранения Краснодарского края, расположенному по адресу: 352007, Краснодарский край, Кущевский район, х. Цукерова Балка, пер. Больничный 7, следующих своих персональных данных (включая получение их от меня и/или любых третьих лиц):

«Фамилия, имя, отчество, информация о смене фамилии, имени, отчества, пол, год, месяц и дата рождения, место рождения, гражданство, документ, удостоверяющий личность (серия, номер, кем и когда выдан), номер и дата трудового договора, заграничный паспорт, водительское удостоверение, место и дата регистрации, место жительства, номера телефонов (городской, мобильный), адрес электронной почты, семейное положение, состав семьи, отношение к воинской обязанности, воинское звание, состав рода войск, военный билет, приписное свидетельство, сведения о наличии детей, их возрасте, месте работы (учебы), сведения о постановке на воинский учет и прохождении службы в Вооруженных Силах, сведения о полученном профессиональном и дополнительном образовании (наименование образовательного учреждения, специальность и квалификация по документу об образовании; документ об образовании, о квалификации, наличии специальных знаний; наименование документа об образовании, его серия и номер; послевузовское профессиональное образование), сведения об уровне профессиональных знаний, о владении специальными умениями и навыками (работа на компьютере, владение иностранными языками и др.), ученая степень (отрасль науки, диплом, диссертационный совет, дата присуждения ученой степени), ученое звание (аттестат, его номер, дата присвоения ученого звания, научная специальность), повышение квалификации, профессиональная переподготовка, сведения о предыдущей трудовой деятельности, трудовая книжка и

сведения, содержащиеся в ней (сведения о продолжительности общего трудового стажа, страхового стажа, непрерывного стажа и др.), сведения о состоянии здоровья и его соответствии выполняемой работе, сведения по отпускам и командировкам, общий медицинский стаж, наличие научных трудов, изобретений, список научных трудов, аттестации, награды (поощрения), взыскания, почетные звания, ИНН, страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), номер страхового полиса (ОМС), профессия, должность, ставка заработной платы в соответствии с профессиональными группами и уровнями, заработная плата, включая все выплаты, наличие и группа инвалидности и степени ограничения способности к трудовой деятельности, наличие судимостей, социальные льготы»
с целью моего трудоустройства, заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений, между мной и Государственным учреждением здравоохранения Краснодарского края «Специализированная психиатрическая больница №3» департамента здравоохранения Краснодарского края, как работодателем, подтверждения этапов и характера моей трудовой деятельности в больнице, его взаимодействия с федеральными органами для совершения сбора, систематизации, накопления, хранения, уточнения, обновления, изменения, использования (в том числе и для получения и передачи), обезличивания, блокирования, уничтожения и трансграничной передачи персональных данных с учетом действующего законодательства с использованием как автоматизированных средств обработки моих персональных данных, так и без использования средств автоматизации.

Настоящее соглашение действует со дня его подписания до дня отзыва в письменной форме, или 75 лет с момента подписания согласия.

В случае неправомерного использования моих персональных данных согласие на обработку персональных данных отзывается моим письменным заявлением.

«_____»_____20___г. _____

(подпись)

Приложение 7 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

СОГЛАСИЕ ПАЦИЕНТА НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____
(фамилия, имя, отчество)
проживающий (ая) по адресу _____

_____

_____

паспорт _____
(серия и номер основного документа, удостоверяющего личность
_____
кем и когда выдан, номер подразделения)

в соответствии с требованиями статьи 9 федерального закона от 27.07.06 г. “О персональных данных” № 152-ФЗ, подтверждаю свое согласие на обработку Государственному бюджетному учреждению здравоохранения «Специализированная психиатрическая больница №3» министерства здравоохранения Краснодарского края, расположенному по адресу: 352007, Краснодарский край, Кущевский район, х. Цукерова Балка, пер. Больничный 7 (далее — Оператор) моих персональных данных, включающих: фамилию, имя, отчество, пол, дату рождения, адрес места жительства, контактный(е) телефон(ы), реквизиты полиса ОМС (ДМС), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), реквизиты документа, удостоверяющего личность, данные о состоянии моего здоровья, заболеваниях, случаях обращения за медицинской помощью — в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну. В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора, в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в информационные системы персональных данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных.

«_____»_____20___г. _____ (подпись)

Приложение 8 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Отзыв согласия на обработку персональных данных

Главному врачу Государственного бюджетного учреждения здравоохранения «Специализированная психиатрическая больница №3» министерства здравоохранения Краснодарского края, расположенного по адресу: 352007, Краснодарский край, Кущевский район, х. Цукерова Балка, пер.Больничный 7

_____ _____
Ф.И.О. субъекта персональных данных
_____

_____ Адрес где
зарегистрирован субъект персональных данных
_____
Номер и серия основного документа, удостоверяющего его личность

_____
Дата выдачи указанного документа
_____
Наименование органа, выдавшего документ

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с_____
(указать причину)

"___"_____ 20__ г. _____ _____
(подпись) (расшифровка подписи)

Приложение 9 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Соглашение работника
о неразглашении персональных данных субъекта

Я, _____, паспорт серии _____,
номер _____, выданный _____
"___"_____ ____ года, понимаю, что получаю доступ к персональным данным работников и/или пациентов ГУЗ КК СПБ №3.

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

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

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в "Положении об обработке и защите персональных данных" требования.

Я подтверждаю, что не имею права разглашать сведения:
- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- 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, их аттестации;
- копии отчетов, направляемые в органы статистики
- содержание медицинской карты пациента.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового кодекса Российской Федерации, федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных», с кодексом об административных правонарушениях Российской Федерации.

"___ " _____ 20__ г. _____
(подпись)

Приложение 10 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Журнал
учета передачи персональных данных

№п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

Приложение 11 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

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

№п/п	Сведения о запрашивающем лице	Краткое содержание обращения	Цель получения информации	Отметка о передаче или отказе в предоставлении информации	Дата передачи/отказа в предоставлении информации	Подпись запрашивающего лица	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

Приложение 12 к
приказу
ГБУЗ СПБ № 3
от 09.01.2018 г. № 152-п

Типовой должностной регламент
специалиста по обеспечению безопасности персональных данных

I. Общие положения

1.1. Настоящий должностной регламент специалиста по обеспечению безопасности персональных данных (далее - Регламент) определяет основные цели, функции и права специалиста по обеспечению безопасности персональных данных (далее - Специалист) в соответствующей организации.
1.2. Специалист назначается приказом (или иным документом) Руководителя организации на основании Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15.09.1993 N 912-51, во исполнение Федерального закона "О персональных данных" N 152-ФЗ от 27.07.2006.
1.3. Специалист проводит свою работу согласно нормативным методическим документам Федеральной службы по техническому и экспортному контролю России, Федеральной службы безопасности России, Роскомнадзора и иных уполномоченных законодательством органов в области обеспечения безопасности персональных данных.
1.4. Непосредственное руководство работой специалиста осуществляет заместитель Руководителя организации, курирующий вопросы защиты информации. Назначение и освобождение от должности специалиста производится Руководителем организации.
1.5. Специалист назначается из числа сотрудников соответствующей организации, имеющих опыт работы по основной деятельности соответствующей организации или в области защиты.
1.6. Специалист приравнивается по оплате труда, льготам и премированию к соответствующим категориям работников основных подразделений соответствующей организации.
1.7. Работа специалиста проводится в соответствии с планами работ, утверждаемыми непосредственным руководителем или руководителем организации.
1.8. В своей работе специалист руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, приказами и указаниям Руководителя организации и другими руководящими документами по обеспечению безопасности персональных данных.

II. Основные функции специалиста

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в соответствующей организации.
2.2. Проведение мероприятий по организации обеспечения безопасности персональных данных, включая классификацию информационных систем персональных данных.
2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в том числе
- мероприятия по размещению, охране, организации режима допуска в помещения, где ведется обработка персональных данных;
- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;
- мероприятия по защите от несанкционированного доступа к персональным данным

- мероприятия по выбору средств защиты персональных данных при их обработке.
2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.
2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.
2.6. Недопущение воздействия на технические средства обработки персональных данных, в результате которого может быть нарушено их функционирование.
2.7. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
2.8. Постоянный контроль за обеспечением уровня защищенности персональных данных.
2.9. Участие в подготовке объектов соответствующей организации к аттестации по выполнению требований обеспечения безопасности персональных данных.
2.10. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в соответствующей организации.
2.11. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.
2.12. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в соответствующей организации.
2.13. Проведение периодического контроля эффективности мер защиты персональных данных в соответствующей организации. Учет и анализ результатов контроля.
2.14. Организация повышения осведомленности руководства и сотрудников в соответствующей организации по вопросам обеспечения безопасности персональных данных, сотрудников подведомственных предприятий, учреждений и организаций.
2.15. Подготовка отчетов о состоянии работ по обеспечения безопасности персональных данных в соответствующей организации.

III. Права специалиста

Специалист имеет право:
3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.
3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.
3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.
3.4. Контролировать деятельность структурных подразделений соответствующей организации в части выполнения ими требований по обеспечению безопасности персональных данных.
3.5. Вносить предложения руководителю организации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.
3.6. Привлекать в установленном порядке необходимых специалистов из числа сотрудников соответствующей организации для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

IV. Ответственность специалиста

4.1. Специалист несет персональную ответственность за:
правильность и объективность принимаемых решений;

правильное и своевременное выполнение приказов, распоряжений, указаний руководства соответствующей организации по вопросам, входящим в возложенные на него функции;
выполнение возложенных на него обязанностей, предусмотренных настоящим Регламентом;
соблюдение трудовой дисциплины, охраны труда;
качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.
согласно действующему законодательству Российской Федерации за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

Л И С Т
ознакомления с Положением
о политике Государственного бюджетного учреждения здравоохранения «Специализированная психиатрическая больница №3»
министерства здравоохранения Краснодарского края (ГБУЗ СПБ № 3) в сфере сбора, обработки и защиты персональных данных работников, пациентов, посетителей

№ п/п	Фамилия, имя, отчество работника	Дата	Подпись работника