УТВЕРЖДАЮ
Главный врач
МУЗ «Городская больница №1»
_____ В.А. Жуков
«___»_____ 2016г

ПОЛИТИКА

обработки и защиты персональных данных
в Муниципальном учреждении здравоохранения
«Городская больница №1»
г. Волгодонска, Ростовской области
(название организации)

г. Волгодонск
2016

Определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

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.

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.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

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.

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.

Доступ к информации – возможность получения информации и ее использования.

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).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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.

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.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

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.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

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.

Оператор (персональных данных) – 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.

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.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

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.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

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.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.
Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.
Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.
Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.
Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.
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.
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.
Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.
Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.
Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).
Обозначения и сокращения
АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации

СЗПДн – система (подсистема) защиты персональных данных
СОВ – система обнаружения вторжений
ТКУ И – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в области обработки и защиты персональных данных (далее – Политика) в Муниципальном учреждении здравоохранения «Городская больница №1» г. Волгодонска, Ростовской области (далее МУЗ «Городская больница №1»), является официальным документом, разработана во исполнение требований ч. 2 ст. 18.1 Федерального закона от 27.07.2006 г. No 152-ФЗ «О персональных данных», а также иных нормативно-правовых актов Российской Федерации в области защиты и обработки персональных данных и действует в отношении персональных данных, которые могут быть получены от субъектов персональных данных.
1.2. При осуществлении уставной деятельности МУЗ «Городская больница №1» (далее – Учреждение) обрабатывает персональные данные. Осуществляя обработку персональных данных (далее - ПДн), Учреждение считает своими важнейшими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных. Учреждение несет ответственность за соблюдение конфиденциальности и безопасности обрабатываемых персональных данных.
1.3. Настоящая Политика определяет основные цели, принципы обработки и меры, применяемые для организации защиты ПДн в Учреждении.
1.4. В Политике раскрываются:
• основные категории персональных данных, обрабатываемых Учреждением;
• цели, способы и принципы обработки Учреждением персональных данных;
• права и обязанности Учреждения при обработке персональных данных;
• права субъектов персональных данных;
• меры, применяемые Учреждением в целях обеспечения безопасности персональных данных при их обработке.
1.5. Настоящая Политика распространяется на все случаи обработки персональных данных Учреждением, вне зависимости от того, является обработка персональных данных автоматизированной или неавтоматизированной, производится она вручную либо автоматически.
1.6. Настоящая Политика является внутренним локальным нормативным актом Учреждения и является обязательной для исполнения всеми подразделениями и работниками Учреждения.
1.7. Каждый работник, вновь принимаемый на работу в Учреждение, во время первого вводного инструктажа должен быть ознакомлен с настоящей Политикой.
1.8. Настоящая Политика утверждается руководителем Учреждения, который осуществляет контроль соблюдения Политики в Учреждении
1.9. Учреждение имеет право вносить изменения в настоящую Политику. Срок действия настоящей Политики - три года после ее утверждения. Политика подлежит пересмотру не реже одного раза в три года. Новая редакция Политики вступает в силу после ее утверждения руководителем Учреждения и подлежит доведению до работников Учреждения и опубликованию в информационно-телекоммуникационной сети в соответствии с ч. 2 ст. 18.1 Федерального закона от 27.07.2006 г. No 152-ФЗ «О персональных данных».
1.10. Ответственность за актуализацию настоящей Политики и текущий контроль над выполнением норм Политики возлагается на Председателя Комиссии по защите персональных данных и иных сведений, составляющих тайну, охраняемую законом, созданной в Учреждении.

1.11. Учреждение разрабатывает все внутренние локальные акты и иные документы, связанные с обработкой ПДн, на основании требований настоящей Политики.
1.12. Настоящая Политика является общедоступным документом. Для обеспечения неограниченного доступа к документу, текст настоящей Политики размещен на общедоступном официальном сайте www.vgb-1.ru

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Принципы обработки персональных данных в Учреждении

2.1.1. Обработка персональных данных в Учреждении осуществляется на основе следующих принципов:
• на законной и справедливой основе;
• должна ограничиваться достижением конкретных, заранее определенных и законных целей;
• не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
• не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
• обработке подлежат только персональные данные, которые отвечают целям их обработки;
• 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;
• должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
• 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 является субъект персональных данных;
• 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;
• обеспечивается защита прав и свобод человека и гражданина при обработке его персональных данных, в том числе защита прав на неприкосновенность частной жизни, личной и семейной тайны.

2.2. Правовые основания обработки персональных данных в Учреждении

2.2.1. Политика Учреждения в области обработки персональных данных определяется в соответствии со следующими нормативными правовыми актами Российской Федерации:
• ст. ст. 23-24 Конституции Российской Федерации;
• часть 4 Гражданского кодекса Российской Федерации от 18.12.2006 г. No 230-ФЗ;
• ст. ст. 86-90 главы 14 Трудового Кодекса Российской Федерации от 30.12.2001 г. No 197-ФЗ;
• ст. 8 Федерального закона от 28.03.1998 г. No 53-ФЗ «О воинской обязанности и военной службе»;
• ст.3, ст. 13, ст. 17, ст.23, ст. 23, ст. 25, ст. 27 Федерального закона от 22.10.2004 г. No 125-ФЗ «Об архивном деле в Российской Федерации»;
• Федеральный закон от 19.12.2005 г. No160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

• ст. ст. 5-6, ст. 15 Федерального закона от 02.05.2006 г, No 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
• ст. 6 Федерального закона от 27.07.2006 г. No 152-ФЗ «О персональных данных»;
• ст. ст. 6-9, ст. ст. 16-17 Федерального закона от 27.07.2006 г. No 149-ФЗ «Об информатизации, информационных технологиях и о защите информации»;
• ст. 28, ст. 32 Федерального закона от 24.07.2009 г. No 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации. Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»;
• Федеральный закон от 21.11.2011 года No 323-ФЗ «Об охране здоровья граждан в Российской Федерации»
• ст. 4 главы 1, ст. 13 главы 2, ст. ст. 14-16 главы 3, глава 4, ст. 55 главы 5, ст. 51, ст. ст. 53-54., ст. 59 главы 6, ст. ст. 91-94, ст. 97 Федерального закона от 21.11.2011 г. No 323- ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
• Постановлением Правительства Российской Федерации от 16.04.2003 г. No 225 «О трудовых книжках»;
• Постановлением Правительства Российской Федерации от 27.11.2006 г. No719 «Об утверждении Положения о воинском учете»;
• Постановлением Правительства Российской Федерации от 06.07.2008 г. No512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиях хранения таких данных вне информационных систем персональных данных»;
• Постановлением Правительства Российской Федерации от 15.09. 2008 г. No 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
• Постановлением Правительства Российской Федерации от 21.03.2012 г. No 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
• Постановлением Правительства Российской Федерации от 01.11. 2012 г. No 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
• Постановлением Министерства труда Российской Федерации от 10.10. 2003 г. No 69 «Об утверждении Инструкции по заполнению трудовых книжек»;
• Приказом Министерства здравоохранения Российской Федерации от 31.12.2013 г. No 1159н «Об утверждении Порядка ведения персонифицированного учета при осуществлении медицинской деятельности лиц, участвующих в оказании медицинских услуг»;
• другими действующими нормативно-правовыми актами Российской Федерации, ФСБ России, ФСТЭК России, Министерства здравоохранения Российской Федерации, ТФОМС, а также приказами и распоряжениями Управления здравоохранения г. Волгодонска, относящимся к вопросу обработки и защиты персональных данных.
• другие нормативно-правовые акты, регламентирующие защиту персональных данных.
2.2.2. Обработка персональных данных не может быть использована Учреждением в целях:
• причинения имущественного и морального вреда гражданам;
• затруднения реализации прав и свобод граждан Российской Федерации.
2.2.3. Обработка персональных данных в Учреждении должна ограничиваться достижением законных, конкретных и заранее определенных целей. Обработке подлежат только те персональные данные, и только в том объеме, которые отвечают целям их обработки.

2.2.4. Все принимаемые в Учреждении локальные нормативные акты, регламентирующие обработку в Учреждении персональных данных, разрабатываются на основании настоящей Политики.

2.3. Цели обработки персональных данных в Учреждении

2.3.1. Учреждение осуществляет обработку персональных данных исключительно в целях:

• осуществления возложенных на Учреждение Уставом и законодательством Российской Федерации функций в соответствии с нормативными актами, указанными в п. 2.2. настоящей Политики;

• формирования единой информационной системы городского здравоохранения путем организации на базе современных компьютерных технологий системы сбора, обработки, хранения и предоставления информации, обеспечивающей динамическую оценку состояния здоровья граждан и информационную поддержку принятия управленческих решений, направленных на его улучшение;

• организации учета работников Учреждения в соответствии с требованиями законов и иных нормативно-правовых актов, содействия им в трудоустройстве и карьерном росте, в обучении, для предоставления им иных льгот и компенсаций;

• принятия решения о заключении с соискателем трудового договора;

• исполнения обязательств Учреждением и осуществление прав Учреждения по заключенным с контрагентами договорам;

• исполнения обязательств Учреждением и осуществление прав Учреждения по заключенным с иными физическими лицами или юридическими лицами договорам в соответствии с нормами Гражданского кодекса Российской Федерации;

• для исполнения Учреждением обязательств и осуществление прав Учреждения в процессе судопроизводства по искам к Учреждению работников, контрагентов, партнеров, субъектов персональных данных или исков Учреждения к работникам, контрагентам, партнерам, субъектам персональных данных в рамках Гражданского процессуального кодекса Российской Федерации, Арбитражного процессуального кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях;

• для исполнения Учреждением обязательств и осуществление прав Учреждения при осуществлении претензионного делопроизводства по жалобам к Учреждению работников, контрагентов, партнеров, субъектов персональных данных или претензий Учреждения к работникам, контрагентам, партнерам, субъектам персональных данных в рамках Гражданского кодекса Российской Федерации, Гражданского процессуального кодекса Российской Федерации, Арбитражного процессуального кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях;

• осуществления пропускного и внутриобъектового режима в помещениях Учреждения.

• оказание медицинских и немедицинских услуг пациентам.

2.3.2. В Учреждении обработке подлежат только те персональные данные, которые отвечают указанным выше целям их обработки. Персональные данные не подлежат обработке в случае несоответствия их характера и объема поставленным целям.

2.3.3. Учреждение не осуществляет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений.

2.3.4. В том случае если для достижения указанных выше целей обработки персональных данных, Учреждению необходимо осуществить обработку биометрических персональных данных, либо данных касающихся состояния здоровья, то такая обработка осуществляется только на основании письменного согласия субъекта персональных данных. Обработка специальных категорий персональных данных, должна быть незамедлительно прекращена, если устранены причины, вследствие которых она осуществлялась.

2.4. Допуск работников Учреждения к обработке персональных данных

2.4.1. Персональные данные в Учреждении могут обрабатываться только уполномоченными в установленном порядке работниками.

2.4.2. Работники допускаются к обработке персональных данных только по решению руководителя Учреждения на основании приказа.
2.4.3. Работники, допущенные в Учреждении к обработке персональных данных, имеют право приступать к работе с персональными данными только после ознакомления под личную роспись с локальными нормативными актами, регламентирующими в Учреждении обработку ПДн, и оформления письменного обязательства о неразглашении сведений конфиденциального характера.
2.4.4. Работники, осуществляющие в Учреждении обработку персональных данных, должны действовать в соответствии с должностными инструкциями, регламентами и другими распорядительными документами Учреждения и соблюдать требования Учреждения по соблюдению режима конфиденциальности персональных данных.

2.5. Получение персональных данных, категории субъектов персональных данных, сроки обработки и хранения персональных данных

2.5.1. Учреждение получает персональные данные только на основании того, что субъект персональных данных принимает решение о предоставлении Учреждению своих персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.
2.5.2. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой форме, позволяющей подтвердить факт его получения.
Как правило, такое согласие дается в письменной форме в соответствии с требованиями ст. 9 ч. 2 Федерального закона от 27.07.2006 г. No 152-ФЗ «О персональных данных».
Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с п. 1 ст. 9 ч. 2 Федерального закона от 27.07.2006 г. No 152-ФЗ «О персональных данных».
2.5.3. Учреждение является оператором, осуществляющим обработку персональных данных в отношении персональных данных следующих физических лиц:
• работников Учреждения, с которыми заключены трудовые договоры, лицами, выполняющими работы в интересах Учреждения в соответствии с заключенными с ними гражданско-правовыми договорами, кандидатов на соискание вакантной должности;
• близкие родственники работников Учреждения
• контрагентов Учреждения, которым Учреждение оказывает услуги;
• представителей контрагентов Учреждения, с которыми у Учреждения существуют договорные отношения или с которыми Учреждение намерено вступить в договорные отношения.
• пациенты, законные представители пациентов,
• посетители Учреждения.
Источники получения персональных данных:
- непосредственно сами субъекты персональных данных (работники, пациенты, посетители, контрагенты и т.д.)
- медицинские организации, страховые медицинские организации, осуществляющие деятельность на территории Ростовской области
- Территориальный фонды обязательного медицинского страхования субъектов Российской Федерации
- Министерство здравоохранения Ростовской области
- органы записи актов гражданского состояния
- отделение Пенсионного фонда Российской Федерации по Ростовской области
- Ростовское региональное отделение Фонда социального страхования Российской Федерации, иные государственные органы и уполномоченные организации в случаях, предусмотренных законодательством Российской Федерации.

2.5.4. Учреждение является юридическим лицом, организующим обработку персональных данных на основании законодательства и по поручению других операторов, к которым относятся (не исчерпывая):
• органы государственной власти;
• федеральные органы исполнительной власти, которым предоставляется отчетность, содержащая персональные данные работников и субъектов персональных данных, в соответствии с законодательством Российской Федерации и нормативно-правовыми актами, принятыми соответствующими органами в рамках их компетенции, а также организациям, предоставление сведений которым предусмотрено нормативно-правовыми актами - в объеме, определенном соответствующими федеральными законами;
• Управления здравоохранения г. Волгодонска;
• Медицинские организации
• Страховые медицинские организации
• Территориальный фонд обязательного медицинского страхования Ростовской области.
2.5.5. Сроки обработки и хранения персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, сроком исковой давности, сроками хранения документов, установленными Приказом Министерства культуры Российской Федерации от 25 августа 2010 года No 558 «Об утверждении перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», иными требованиями законодательства и нормативными документами, а также сроком предоставленного субъектом согласия на обработку персональных, в случаях, когда такое согласие должно быть предоставлено в соответствии с требованиями законодательства.
2.5.6. Учреждение осуществляет обработку персональных данных путем сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, передачи, обезличивания, блокирования, уничтожения.
2.5.7. В Учреждении используется смешанный (с использованием средств автоматизации) способ обработки персональных данных с передачей информации по внутренней локальной сети и с передачей информации по сети Интернет в защищенном режиме.
2.5.8. Учреждение осуществляет обработку специальных категорий персональных данных, касающихся состояния здоровья и биометрических персональных данных (фотографическое изображение).
2.5.9. Обработка специальных категорий персональных данных.
Учреждение обрабатывает специальную категорию персональных данных - состояние здоровья субъекта персональных данных (врачебная тайна). Разглашение врачебной тайны, в том числе регулируется Федеральным законом No 323-ФЗ от 21 ноября 20011 года «Об основах охраны здоровья граждан в Российской Федерации» (ст. 13 Закона).
Обработка специальной категории персональных данных в Учреждении возможна в следующих случаях:
- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных
- персональные данные сделаны общедоступными субъектом персональных данных
- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- 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;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских услуг при условии,

что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с действующим законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обороне, безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, об исполнительном производстве, уголовно-исправительньм законодательством Российской Федерации;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации об обязательных и добровольных видах страхования, со страховым законодательством Российской Федерации.

2.6. Передача персональных данных третьим лицам

2.6.1. Передача персональных данных третьим лицам осуществляется Учреждением исключительно для достижения целей, заявленных для обработки персональных данных в п. 3.3. настоящей статьи Политики.
2.6.2. Передача персональных данных третьим лицам осуществляется либо с письменного согласия субъекта персональных данных, которое оформляется по установленной законодательством форме, либо для исполнения договора, стороной которого или выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем, либо в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, либо в иных случаях, установленных федеральным законодательством.
2.6.3. Передача персональных данных третьим лицам осуществляется Учреждением только на основании соответствующего договора с третьим лицом, существенным условием которого является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.
2.6.4. Учреждение не осуществляет трансграничную передачу персональных данных субъектов персональных данных на территории иностранных государств.
2.6.5. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных Учреждения в ходе своей деятельности предоставляет персональные данные следующим третьим лицам:
2.6.5.1. персональные данные работников на основании трудового договора и/или письменного согласия передаются в нижеследующие организации:
• кредитным организациям, в которые работники обращались для оформления кредитов, ссуд либо получения иных услуг, при условии, что работники заранее сообщат работодателю наименования указанных кредитных организаций;
• полиграфической организации или типографии - для изготовления визитных карточек работника, при условии, что Учреждение заранее сообщит им наименование и адрес данного полиграфического предприятия;
• частной охранной организации, осуществляющей охрану помещений, при условии, что Учреждение заранее сообщит работнику наименование и адрес данной частной охранной организации;
• партнерам Учреждения - для исполнения обязательств, возложенных на Учреждение договорами и иными законными сделками, исполнение которых предусмотрено должностными обязанностями работника, при условии, что Учреждение заранее сообщит работнику наименования и адреса данных организаций.
• налоговым органам и правоохранительным органам, подразделениям Пенсионного фонда Российской Федерации, подразделениям Федеральной миграционной службы

России, центрам занятости населения, военкоматам - для исполнения обязательств, возложенных на Учреждение законодательными и нормативными актами, а также исполнения законных официальных запросов, касающихся работника.
• другим организациям и органам в соответствии с законодательством РФ.
2.6.5.2. персональные данные контрагентов в соответствии с заключенным с ними Учреждением или партнерами письменным договором, и/или с письменного согласия субъекта персональных Учреждение на основании договоров передает нижеследующим третьим лицам:
• налоговым и правоохранительным органам - для исполнения обязательств, возложенных на Учреждение законодательными и нормативными актами, а также исполнения законных официальных запросов, касающихся контрагентов.
• другим организациям и органам в соответствии с законодательством Российской Федерации

2.7. Получение Учреждением в качестве третьего лица персональных данных от партнеров

2.7.1. Получение персональных данных от партнеров - операторов персональных данных, - осуществляется Учреждением исключительно для достижения целей, заявленных для обработки персональных данных в п. 2.3. настоящей статьи Политики, и на основании заключенных с партнерами письменных договоров.
2.7.2. В тексте договоров с партнерами обязательно определяются цели обработки персональных данных, перечень операций с ними, и устанавливается обязанность Учреждения соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указываются требования к защите обрабатываемых персональных данных.
2.7.3. Учреждение, осуществляя обработку персональных данных по поручению партнера, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В этом случае ответственность перед субъектом персональных данных за действия Учреждения несет партнер. Учреждение, осуществляя обработку персональных данных по поручению партнера, несет ответственность перед партнером.

2.8. Меры по обеспечению безопасности персональных данных при их обработке

2.8.1. До начала обработки персональных данных Учреждением предприняты правовые, технические и организационные меры к защите персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:
• вводом в Учреждении режима конфиденциальности персональных данных, когда все документы и сведения, содержащие информацию о персональных данных, являются в Учреждении конфиденциальными;
• организацией режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
• утверждением полного перечня персональных данных и иных сведений, подлежащих защите в Учреждении;
• обеспечением не распространения документов и сведений, содержащих персональные данные, без согласия субъекта персональных данных, либо наличия иного законного основания;
• назначением уполномоченного сотрудника, ответственного за организацию обработки персональных данных;

• введением персональной ответственности руководителей Учреждения и его подразделений за обеспечение режима безопасности персональных данных при их обработке;
• утверждением перечня лиц, осуществляющих в Учреждении обработку персональных данных либо имеющих к ним доступ;
• определением типа угроз безопасности персональных данных актуальных для информационных систем Учреждения с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных;
• разработкой и утверждением локальных нормативных актов, регламентирующих в Учреждении обязанности должностных лиц, осуществляющих обработку и защиту персональных данных, их ответственность за компрометацию персональных данных;
• осуществлением внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 г. No 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам;
• запретом для работников, осуществляющих обработку персональных данных, проводить несанкционированное или нерегистрируемое копирование персональных данных, в том числе с использованием сменных носителей информации, мобильных устройств копирования и переноса информации, коммуникационных портов и устройств ввода-вывода, реализующих различные интерфейсы (включая беспроводные), запоминающих устройств мобильных средств (например, ноутбуков, карманных персональных компьютеров, смартфонов, мобильных телефонов), а также устройств фото и видеосъемки;
• обеспечением сохранности носителей персональных данных;
• использованием 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;
• ознакомлением работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных сотрудников;
• выделением конкретных мест хранения персональных данных (материальных носителей), обработка которых осуществляется Учреждением и организацией режима обеспечения безопасности помещений и мест хранения материальных носителей персональных данных;
• обеспечением раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется без использования средств автоматизации и в различных целях;
• осуществлением учета документов по обработке персональных данных без использования автоматизированных систем отдельным делопроизводством, хранением документов в надежно запираемых шкафах и сейфах, ключи от которых хранятся только у ответственных за данную деятельность работников.
• определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
• применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;
• оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
• учетом машинных носителей персональных данных;

• выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер;
• восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
• установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
• обеспечением доступа к содержанию электронного журнала событий исключительно уполномоченных работников Учреждения, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения трудовых обязанностей;
• контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

2.9. Права и обязанности субъекта персональных данных.

2.9.1. Субъект персональных данных имеет право:
• на получение сведений об Учреждении, о месте его нахождения, о наличии у Учреждения персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;
• требовать от Учреждения 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;
• требовать прекращения обработки своих персональных данных;
• получать информацию, касающуюся обработки его персональных данных, в том числе содержащую: подтверждение факта обработки персональных данных Учреждением, а также цель такой обработки; способы обработки персональных данных, применяемые Учреждением; сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ; перечень обрабатываемых персональных данных и источник их получения; сроки обработки персональных данных, в том числе сроки их хранения; сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

2.9.2. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в следующих случаях:
• если обработка персональных данных, включая те, что получены в результате оперативно розыскной, контрразведывательной и разведывательной деятельности, выполняется в целях укрепления обороны страны, обеспечения безопасности государства и охраны правопорядка;
• при условии, что обработка персональных данных производится органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
• если обработка персональных данных выполняется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
• когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

• если 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.

2.9.3. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться в Учреждение. Учреждение рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

2.9.4. Субъект персональных данных вправе обжаловать действия или бездействие Учреждения путем обращения в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор).

2.9.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке.

2.9.6. Субъект персональных данных обязан предоставлять только достоверные и полные персональные данные, которые при необходимости должны быть документально подтверждены.

2.10. Порядок предоставления информации субъекту персональных данных

2.10.1. Доступ к персональным данным субъекту персональных данных или его законному представителю предоставляется Учреждением при обращении либо при получении запроса от субъекта персональных данных или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

2.10.2. Учреждение сообщает субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

2.10.3. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

2.10.4. Неправомерный отказ в предоставлении собранных в установленном порядке документов, содержащих персональные данные, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации может повлечь наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

2.11. Ответственность за обеспечение безопасности персональных данных

2.11.1. Учреждение несет ответственность за разработку, введение и действенность соответствующих требованиям законодательства норм, регламентирующих получение, обработку и защиту персональных данных. Общество закрепляет персональную ответственность работников за соблюдением установленного в Учреждении режима конфиденциальности персональных данных.

2.11.2. Руководитель подразделения несет персональную ответственность за соблюдение работниками его подразделения норм, регламентирующих получение, обработку и защиту персональных данных. Руководитель, разрешающий доступ сотрудника к документам и сведениям, содержащим персональные данные, несет персональную ответственность за данное разрешение.
2.11.3. Каждый работник Учреждения, получающий для работы документ, содержащий персональные данные, несет персональную ответственность за сохранность носителя и конфиденциальность информации.
2.11.4. Работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.
2.11.5. Учреждение не несет ответственности за убытки и иные затраты, понесенные субъектами персональных данных в результате предоставления ими недостоверных и неполных персональных данных.

3. СВЕДЕНИЯ ОБ УЧРЕЖДЕНИИ

Полное наименование: Муниципальное учреждение здравоохранения «Городская больница № 1» г. Волгодонск, Ростовской области
Сокращенное наименование: МУЗ «Городская больница №1»
Главный врач: Жуков В.А.
Адрес местонахождения: пер. Первомайский, 46/45, г. Волгодонск
Почтовый адрес: 347360, Ростовская область, г. Волгодонск, пер. Первомайский, 46/45
Телефон: 8 (8639) 22-23-09
Факс: 8 (8639)22-23-09
E-mail: vgb1@mail.ru
Персональный сайт: vgb-1.ru
Учреждение является оператором персональных данных.

4. СВЕДЕНИЯ ОБ УПОЛНОМОЧЕННОМ ОРГАНЕ ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Федеральная служба по надзору в сфере связи, информационных технологий и массовых комму
никаций (Роскомнадзор)
Почтовый адрес: 109074, г. Москва, Китайгородский пр., д.7, стр.2. Справочно-информационный
центр: телефон (495) 987-68-00, факс (495) 987-68-01. Управление Роскомнадзора по защите прав
субъектов персональных данных: тел.: (495) 987-68-57.
Общий электронный адрес (E-mail): rsoc in@rsoc.ru Сайт: pd.rkn.gov.ru
4.2. Управлении Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ростовской области
Адреса

Юридический:	Металлургическая ул., 113/46, г. Ростов-на-Дону, 344029
Почтовый:	Металлургическая ул., 113/46, г. Ростов-на-Дону, 344029
Электронная почта:	rsockanc61@rkn.gov.ru Сайт: 61.rkn.gov.ru

СОГЛАСОВАНО

Ответственный за обеспечение безопасности
персональных данных