УТВЕРЖДАЮ
Главный врач
ГБУЗ ГКБ им. С.П. Боткина

_____ / А.В. Шабунин
«10» сентября 2018 г.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных ГБУЗ ГКБ им. С.П. Боткина

Листов: 26

Москва, 2018 г.

ОГЛАВЛЕНИЕ

Термины и определения 3

Условные обозначения и сокращения 4

1. Общие положения 5

1.1. Назначение документа 5

1.2. Цели и задачи 5

1.3. Нормативные ссылки 5

1.4. Область действия 6

1.5. Утверждение и пересмотр 6

2. Обработка персональных данных 6

2.1. Принципы обработки персональных данных 6

2.2. Общий порядок обработки 7

2.3. Получение (сбор) персональных данных 7

2.4. Доступ к персональным данным 8

2.5. Обработка персональных данных без использования средств автоматизации 9

2.6. Передача персональных данных 11

2.7. Порядок уничтожения персональных данных 12

2.8. Особенности обработки персональных данных работников Оператора 12

3. Обязанности лиц, допущенных к обработке персональных данных 13

4. Обеспечение безопасности персональных данных 16

4.1. Принципы обеспечения безопасности персональных данных 16

4.2. Меры по обеспечению безопасности персональных данных 16

4.3. Порядок осуществления взаимодействия, сопровождающего предоставление персональных данных 18

5. Права субъектов на защиту своих персональных данных 18

6. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных 19

7. Контроль выполнения требований настоящего Положения 20

Приложение № 1 Журнал учета ознакомления должностных лиц с правилами обеспечения безопасности персональных данных ГБУЗ ГКБ им. С.П. Боткина 21

Приложение № 2 Обязательство о неразглашении персональных данных 22

Приложение № 3 Соглашение о неразглашении конфиденциальной информации 23

Термины и определения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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

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.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Субъект персональных данных – физическое лицо, индивидуальный предприниматель или представитель юридического лица, заключившее с Оператором гражданский договор на выполнение работ, оказание услуг в соответствии с осуществляемыми Оператором видами деятельности, а также работники Оператора и работники контрагентов Оператора.

Условные обозначения и сокращения

ФСТЭК	–	Федеральная служба по техническому и экспортному контролю РФ
ИСПДн	–	информационная система персональных данных
ПДн	–	персональные данные
РФ	–	Российская Федерация
ФИО	–	фамилия, имя, отчество
КЗ	–	контролируемая зона

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение документа

Положение об обработке и защите персональных данных (далее - Положение) разработано в соответствии с пп. 2 ч.1 статьи 18.1 Федерального закона от 27 июля 2006 года № 152 «О персональных данных» и определяет порядок сбора, хранения, передачи и иных операция (действий) с персональными данными в ГБУЗ ГКБ им. С.П. Боткина (далее - Оператор), устанавливает требования к обработке и защите персональных данных, определяет права, обязанности и ответственность руководителей структурных подразделений и работников Оператора.

1.2. Цели и задачи

Целями настоящего Положения являются:

- определение порядка обработки персональных данных;
- обеспечение соответствия порядка обработки персональных данных законодательству Российской Федерации;
- обеспечение защиты персональных данных.

Задачами настоящего Положения являются:

- определение принципов обработки персональных данных;
- определение условий обработки персональных данных, способов защиты персональных данных;
- определение прав субъектов персональных данных, прав и обязанностей Оператора при обработке персональных данных.

1.3. Нормативные ссылки

1. Трудовой кодекс Российской Федерации от 30 декабря 2001 года № 197-ФЗ;
2. Федеральный закон от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 27 июля 2006 года № 152 «О персональных данных»;
4. Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты российской федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;
5. Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

7. Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Область действия

Действие настоящего Положения распространяется на персональные данные, обрабатываемые Оператором как с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, так и без использования таких средств.

Все работники Оператора, допущенные к работе с персональными данными, в обязательном порядке должны быть ознакомлены с настоящим Положением под подпись в «Журнале учета ознакомления должностных лиц с правилами обеспечения безопасности персональных данных» (Приложение № 1).

1.5. Утверждение и пересмотр

Настоящее Положение вступает в силу с момента его утверждения Главным врачом и действует бессрочно до замены его новым Положением.

Пересмотр Положения производится в следующих случаях:

- при изменении процессов и технологий обработки персональных данных;
- по результатам проверок органа по защите прав субъектов персональных данных, выявившим несоответствия требованиям законодательства РФ по обеспечению безопасности персональных данных;
- при изменении требований законодательства РФ к порядку обработки и обеспечению безопасности персональных данных;
- в случае выявления существенных нарушений по результатам внутренних проверок системы защиты персональных данных.

Ответственным за пересмотр данного Положения является работник Оператора, назначенный ответственным за организацию обработки персональных данных. Измененное Положение утверждается приказом Главного врача.

В соответствии с ч. 2 статьи 18.1 Федерального закона от 27 июля 2006 года № 152 «О персональных данных» обеспечение неограниченного доступа к Положению реализуется путем его публикации на сайте Оператора в сети Интернет, либо иным способом.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Принципы обработки персональных данных

Обработка персональных данных Оператором осуществляется на основании следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;

- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональных данные, обработка которых осуществляется в целях, несовместных между собой;
- обработке подлежат только те персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточными по отношению к заявленным целям обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к заявленным целям их обработки;
- персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Оператор в своей деятельности исходит из того, что субъект персональных данных предоставляет точную и достоверную информацию, во время взаимодействия с Оператором извещает представителей Оператора об изменении своих персональных данных.

2.2. Общий порядок обработки

Приказом Главного врача назначается лицо, ответственное за организацию обработки персональных данных.

Работники Оператора допускаются к обработке персональных данных в том объёме, в котором это необходимо для выполнения должностных обязанностей.

При определении объема и содержания, обрабатываемых персональных данных Оператор руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152 «О персональных данных» и другими нормативными актами. Объем и содержание, обрабатываемых персональных данных, способы обработки персональных данных, должны соответствовать целям обработки персональных данных.

Все документы, содержащие персональные данные, должны быть уничтожены в соответствии с установленным порядком по достижении заявленных целей обработки персональных данных, в случае истечения срока обработки персональных данных, установленного при сборе ПДн, а также в случае отзыва согласия субъекта персональных данных, если отсутствуют иные законные основания обработки персональных данных.

2.3. Получение (сбор) персональных данных

Персональные данные следует получать лично у субъекта персональных данных. Если персональные данные возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено подтверждение согласия в письменном виде, если иное не предусмотрено

федеральным законом. Оператор должен сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

Оператор освобождается от обязанности предоставить субъекту персональных данных указанные выше сведения в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
- персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- предоставление субъекту персональных данных указанных выше сведений нарушает права и законные интересы третьих лиц.

Запрещается требовать от лиц, поступающих на работу, документы, помимо предусмотренных Трудовым кодексом Российской Федерации, иными федеральными законами, указами Президента РФ и Постановлениями Правительства РФ.

Запрещается запрашивать информацию о состоянии здоровья субъекта персональных данных, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

Оператор не имеет права получать и обрабатывать персональные данные субъекта персональных данных о его политических, религиозных, философских и иных убеждениях, а также частной жизни, без его согласия в письменной форме. Оператор не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым Кодексом РФ или иными федеральными законами.

Запрещается принятие решений на основании исключительно автоматизированной обработки персональных данных в случае, если такое решение порождает юридические последствия в отношении субъекта персональных данных.

2.4. Доступ к персональным данным

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах Оператора, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании

перечня, утвержденного Приказом Главным врачом, и только после подписания письменного согласия о соблюдении конфиденциальности персональных данных и соблюдении правил их обработки (Приложение № 2).

Работники, имеющие доступ к персональным данным, имеют право получать и обрабатывать только те персональные данные, которые необходимы им для выполнения конкретных трудовых функций.

В случае если на основании договоров на оказание услуг, заключенных с юридическими и физическими лицами, Оператору необходимо предоставить таким лицам доступ к персональным данным, обрабатываемым Оператором, то соответствующие данные предоставляются Оператором только после подписания с ними соглашения о неразглашении конфиденциальной информации (Приложение № 3) или включения в договоры пунктов о неразглашении конфиденциальной информации, в том числе предусматривающих защиту персональных данных.

Государственным органам, осуществляющим функции контроля (надзора) предоставляют права доступа к персональным данным, обрабатываемым Оператором, только в сфере их компетенции и в объеме, предусмотренном действующим законодательством.

Субъект персональных данных, данные о котором обрабатываются Оператором, имеет право на свободный доступ к своим персональным данным, получение копий своих персональных данных (за исключением случаев, предусмотренных федеральным законом) на основании его письменного запроса.

Оператор обязан в порядке, предусмотренном Федеральным законом от 27 июля 2006 года № 152 «О персональных данных», сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя, либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

2.5. Обработка персональных данных без использования средств автоматизации

Работники Оператора, осуществляющие обработку персональных данных без использования средств автоматизации должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются 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).

При обработке персональных данных без использования средств автоматизации не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий

персональных данных для каждой категории персональных данных должен использоваться отдельный материальный носитель.

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

- типовая форма или связанные с ней документы (инструкции по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта персональных данных, 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;

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

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

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

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

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

- персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию Оператора.

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, предпринимаются меры по обеспечению раздельной обработки персональных данных, в частности:

- 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;

- 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.

Данные правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

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

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна производиться таким образом, чтобы можно было определить места хранения персональных данных (материальных носителей).

2.6. Передача персональных данных

Запрещается передавать персональные данные субъекта третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных законодательством РФ.

Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи, а также представителям субъекта только с письменного разрешения самого субъекта, за исключением случаев, когда передача персональных данных субъекта без его согласия допускается действующим законодательством РФ.

Документы, содержащие персональные данные субъекта, могут быть отправлены в сторонние организации через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные, вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное ее разглашение законодательством предусмотрена ответственность. Далее, конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

Допускается передача персональных данных субъекта без получения его согласия между структурными подразделениями внутри Оператора в объеме, необходимом для выполнения подразделениями своих функций. Лица, получающие персональные данные,

должны быть предупреждены, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены.

Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности (данное требование не распространяется на обмен персональными данными субъектов персональных данных в порядке, установленном федеральным законодательством).

2.7. Порядок уничтожения персональных данных

Уничтожение документов, содержащих персональные данные, производится:

- в случае отзыва согласия субъекта персональных данных, если отсутствуют иные законные основания обработки персональных данных;
- по достижении целей их обработки согласно номенклатуре дел и документов;
- по достижении окончания срока хранения персональных данных, оговоренного в соответствующем соглашении заинтересованных сторон;
- в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.

Уничтожение персональных данных, находящихся на машинных носителях информации, выполняется средствами информационной системы (операционной системы, системы управления базами данных).

Уничтожение материальных носителей с персональными данными осуществляется согласно «Регламенту организации обращения с защищаемыми носителями информации ГБУЗ ГКБ им. С.П. Боткина».

Уничтожение производится по мере необходимости, в зависимости от объемов, накопленных для уничтожения документов. Уничтожение материальных носителей и информации на материальных носителях производится Комиссией по защите персональных данных, назначенной приказом Главного врача. По результатам уничтожения оформляется акт. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

2.8. Особенности обработки персональных данных работников Оператора

В личное дело работника вносятся его персональные данные и иные сведения, связанные с поступлением на работу, ее прохождением, увольнением и необходимые для обеспечения деятельности Оператора.

Личные дела работников находятся в структурном подразделении Оператора, осуществляющим ведение личных дел работников (далее - Отдел кадров) в специально отведенном месте, обеспечивающем защиту от несанкционированного доступа.

К личному делу приобщаются:

- заявление о приеме на работу;
- копия паспорта;

- копии свидетельств о государственной регистрации актов гражданского состояния;
- копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);
- копии приказов о переводах, перемещениях, поощрениях, награждении государственными наградами, присвоении почетных званий, присуждении государственных премий, наложении дисциплинарных взысканий до снятия или отмены (если таковые имеются);
- экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений о внесении изменений и дополнений в трудовой договор;
- копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);
- данные аттестаций;
- копия страхового свидетельства обязательного пенсионного страхования;
- копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;
- копия страхового медицинского полиса обязательного медицинского страхования граждан.

В обязанности Отдела кадров Оператора, осуществляющего ведение личных дел работников, входит:

- приобщение документов к папкам работников;
- обеспечение сохранности папок работников;
- обеспечение конфиденциальности сведений в соответствии с Федеральным законом от 27 июля 2006 года №152 «О персональных данных», другими федеральными законами, иными нормативными правовыми актами Российской Федерации, а также в соответствии с настоящим Положением.

Личное дело ведется на протяжении всей трудовой деятельности работника Оператора.

Сроки хранения персональных данных работников определяются Оператором на основании трудового законодательства Российской Федерации.

3. ОБЯЗАННОСТИ ЛИЦ, ДОПУЩЕННЫХ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных» должностные лица Оператора обязаны:

- знать и выполнять требования настоящего Положения;

- осуществлять обработку персональных данных с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных»;
- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом № 152-ФЗ «О персональных данных»;
- предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, в соответствии с которыми такое согласие не требуется;
- в случаях, предусмотренных Федеральным законом № 152-ФЗ «О персональных данных» осуществлять обработку персональных данных только с согласия в письменной форме субъекта персональных данных;
- предоставлять субъекту персональных данных по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ в предоставлении указанной информации и дать в письменной форме мотивированный ответ, содержащий ссылку на положения Федерального закона № 152-ФЗ «О персональных данных», 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. При обращении либо при получении запроса субъекта персональных данных или его представителя предоставить субъекту персональных данных или его представителю информацию, касающуюся обработки его 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;
- если предоставление персональных данных является обязательным в соответствии с Федеральным законом, разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Описание принимаемых мер приведено в п. 7 настоящем Положении;
- по требованию субъекта персональных данных внести изменения в обрабатываемые персональные данные, или уничтожить их, если персональные данные являются неполными, неточными, неактуальными, незаконно полученными или не являются необходимыми для заявленной цели обработки в срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих

указанные факты, а также 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. Вести Журнал учета обращений субъектов персональных данных, в котором должны фиксироваться запросы субъектов персональных данных на получение персональных данных, а также факты предоставления персональных данных по этим запросам;

- уведомлять субъекта персональных данных об обработке персональных данных в том случае, если персональные данные были получены не от субъекта персональных данных. Исключение составляют следующие случаи:
    - субъект персональных данных уведомлен об осуществлении обработки его персональных данных Оператором;
    - персональные данные получены Оператором на основании Федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
    - персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
    - Оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
    - предоставление субъекту персональных данных сведений, содержащихся в Уведомлении об обработке персональных данных, нарушает права и законные интересы третьих лиц.
- в случае выявления неправомерной обработки персональных данных или неточных персональных данных, устранить выявленные нарушения в соответствии с порядком и сроками, установленными частями 1-3 и 6 Федерального закона № 152-ФЗ «О персональных данных»;
- в случае достижения целей обработки персональных данных незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные 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 Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных №152-ФЗ «О персональных данных» или другими Федеральными законами;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных;
- в случае поступления требования субъекта о прекращении обработки персональных данных в целях продвижения товаров, работ, услуг на рынке немедленно прекратить обработку персональных данных.

4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Принципы обеспечения безопасности персональных данных

Защита персональных данных субъектов от неправомерного использования или утраты обеспечивается Оператором в установленном действующим законодательством и локальными актами Оператора порядке, выполнением комплекса организационных и технических мер, обеспечивающих их безопасность.

Меры по обеспечению безопасности персональных данных при их обработке распространяются как на обработку персональных данных с использованием средств автоматизации, так и без их использования.

Для осуществления мероприятий по обеспечению безопасности персональных данных приказом Главного врача назначаются ответственные лица за обеспечение безопасности персональных данных.

Организацию защиты персональных данных в подразделениях обеспечивают руководители подразделений.

Получение и обработка уполномоченными лицами персональных данных производится после подписания субъектом персональных данных согласия в случаях, если это требуется законодательством.

4.2. Меры по обеспечению безопасности персональных данных

Хранение персональных данных в структурных подразделениях Оператора, работники которых имеют допуск к персональным данным, осуществляется в порядке, исключающем к ним доступ третьих лиц. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

Оператор принимает необходимые и достаточные организационные и технические меры для защиты персональных данных субъектов от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ней третьих лиц.

Оператором применяются следующие методы и способы обеспечения безопасности персональных данных:

- определяются угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;
- применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;
- проводиться оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- ведется учет машинных носителей персональных данных;
- организовывается обнаружение фактов несанкционированного доступа к персональным данным и принятие мер по выявленным нарушениям;
- производится восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- устанавливаются правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивается регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных действий;
- производится контроль за принимаемыми мерами по обеспечению безопасности персональных данных и контроль уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных.

Помещения, в которых ведется обработка персональных данных, должны обеспечивать их сохранность, исключать возможность бесконтрольного проникновения в них посторонних лиц.

По окончании рабочего времени помещения, предназначенные для обработки персональных данных, должны быть закрыты на ключ, бесконтрольный доступ в такие помещения должен быть исключен.

Доступ к информационным системам персональных данных защищается системой паролей. Доступ с мобильных устройств к ресурсам Оператора запрещен.

При взаимодействии с информационными системами сторонних организаций (внешние информационные системы) правила обеспечения защиты ПДн определяются соответствующими организациями (инициаторами передачи). Иная передача ПДн по каналам связи, имеющим выход за пределы КЗ, не осуществляется.

4.3. Порядок осуществления взаимодействия, сопровождающего предоставление персональных данных

В целях обеспечения безопасности персональных данных при взаимоотношении Оператора с третьими лицами должны выполняться следующие меры:

- должно быть подписано соглашение о неразглашении персональных данных;
- должен проводиться мониторинг действий третьих лиц в информационных системах персональных данных Оператора;
- необходимо предусмотреть в договорах с третьими лицами право Оператора на проведение аудита обеспечения защиты персональных данных, передаваемых Оператором третьему лицу.

В случае заключения с юридическим лицом договора, одним из условий которого является передача юридическому лицу персональных данных, обрабатываемых Оператором на законных основаниях, Оператор должен удостовериться до заключения договора в адекватном уровне обеспечения юридическим лицом безопасности персональных данных. Обязательным является наличие доказательств выполнения действующего законодательства РФ по защите персональных данных.

Любое соединение с внешней информационной системой должно быть согласовано с Ответственным за обеспечение безопасности персональных данных. Любой доступ должен быть ограничен и протестирован на возможные уязвимости. Необходимо применять принцип многоуровневой защиты (несколько уровней брандмауэров, отключение протоколов и т.д.). Внешний доступ должен также отвечать следующим характеристикам:

- необходимо подписание владельцем внешней информационной системы соглашения о принятии на себя обязательств по обеспечению безопасности персональных данных в своей части сети, соединенной с сетью Оператора;
- должен быть обеспечен контроль доступа и аутентификация.

5. ПРАВА СУБЪЕКТОВ НА ЗАЩИТУ СВОИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях обеспечения защиты своих персональных данных субъект имеет право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных Федеральным законом;
- определять своих представителей для защиты своих персональных данных;
- требовать исключения или исправления неверных, неполных персональных данных, а также данных, обработанных с нарушением Федерального закона (субъект персональных данных, при отказе Оператора или уполномоченного лица исключить или исправить персональные данные, имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом

такое несогласие; персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения);

- требовать от Оператора или уполномоченного лица уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в суде любые неправомерные действия или бездействие руководителя организации или уполномоченного им лица при обработке и защите персональных данных.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Должностные лица, имеющие доступ к персональным данным, несут личную ответственность за нарушение режима защиты персональных данных в соответствии с законодательством Российской Федерации.

Каждый работник Оператора, получающий для работы содержащий персональные данные документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Работники Оператора, которым персональные данные стали известны в силу их служебного положения, несут ответственность за их разглашение.

Обязательства по соблюдению конфиденциальности персональных данных остаются в силе и после окончания работы с ними вышеуказанных лиц.

За неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей по соблюдению установленного порядка работы с персональными данными работодатель вправе применять предусмотренные Трудовым Кодексом РФ дисциплинарные взыскания.

Ответственность за несоблюдение вышеуказанного порядка обработки персональных данных несет работник, а также руководитель структурного подразделения, осуществляющего обработку персональных данных.

Должностные лица, в обязанность которых входит обработка персональных данных работников Оператора, обязаны обеспечить каждому работнику, при необходимости, возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях РФ.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном федеральным законодательством РФ в области защиты персональных данных.

7. КОНТРОЛЬ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

Повседневный контроль порядка обращения с персональными данными осуществляют руководители тех структурных подразделений Оператора, в которых обрабатываются персональные данные субъектов.

Периодический контроль выполнения настоящего Положения возлагается на должностное лицо, назначенное Главным врачом, ответственное за организацию обработки персональных данных.

ПРИЛОЖЕНИЕ № 1

ЖУРНАЛ УЧЕТА ОЗНАКОМЛЕНИЯ ДОЛЖНОСТНЫХ ЛИЦ С ПРАВИЛАМИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБУЗ ГКБ ИМ. С.П. БОТКИНА

№ п/п	ИНСТРУКТАЖ ПОЛУЧИЛ				ИНСТРУКТАЖ ПРОВЕЛ		
	Фамилия И.О.	Занимаемая должность	Отделение	Подпись	Фамилия И.О.	Подпись	Дата
1							
2							
3							

ПРИЛОЖЕНИЕ № 2

ОБЯЗАТЕЛЬСТВО О НЕРАЗГЛАШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____, паспорт серии _____, номер _____, выданный_____ "___"_____ года, понимаю, что получаю доступ к персональным данным:

- работников ГБУЗ ГКБ им. С.П. Боткина;
- субъектов, не являющихся работниками ГБУЗ ГКБ им. С.П. Боткина.

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься обработкой 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 обработке персональных данных соблюдать все описанные в «Положении об обработке и защите персональных данных ГБУЗ ГКБ им. С.П. Боткина» требования.

Я подтверждаю, что не имею права разглашать сведения, составляющие персональные данные.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я могу быть привлечен(а) к дисциплинарной и материальной ответственности в порядке, установленном в Трудовом кодексе РФ и иными федеральными законами, а также привлечен(а) к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

«___» _____ 20__ г. _____ /_____
(подпись) *(расшифровка подписи)*

ПРИЛОЖЕНИЕ № 3

СОГЛАШЕНИЕ О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

г. Москва "__" _____ 20__ г.

Государственное бюджетное учреждение здравоохранения города Москвы Государственная клиническая больница им. С.П. Боткина Департамента здравоохранения города Москвы (далее – ГБУЗ ГКБ им. С.П. Боткина), далее именуемое «Сторона-1», в лице _____, действующего на основании _____, с одной стороны и

_____, далее именуемое «Сторона-2», в лице _____, действующего на основании _____, с другой стороны, далее совместно именуемые «Стороны»

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», в связи с _____, заключили настоящее Соглашение (далее – Соглашение) о нижеследующем:

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Соглашением регулируются отношения между Сторонами, связанные с обработкой сведений конфиденциального характера, осуществляемой с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, в отношении которых одной из Сторон Соглашения установлен режим конфиденциальности, а также обязанности и ответственность Принимающей Стороны в области защиты сведений конфиденциального характера.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В целях настоящего Соглашения используются следующие основные термины:

- информация - сведения (сообщения, данные) независимо от формы их представления;
- информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
- информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
- информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;
- обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или

ограничивать доступ к информации, определяемой по каким-либо признакам;

- доступ к информации - возможность получения информации и ее использования;
- конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
- предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;
- распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

2.2. Передающая сторона - Сторона Соглашения, передающая в рамках настоящего Соглашения сведения конфиденциального характера.

2.3. Принимающая сторона - Сторона Соглашения, которой были переданы сведения конфиденциального характера.

3. ОБЛАСТЬ ПРИМЕНЕНИЯ

3.1. Настоящее Соглашение применимо ко всем сведениям конфиденциального характера, переданным одной Стороной другой Стороне, или ставшим известным одной из Сторон, в связи с реализацией совместных проектов и исполнением совместных договоров. Настоящее Соглашение применимо ко всем Сторонам данного соглашения, включая дополнительные филиалы и (или) дочерние компании.

3.2. Конфиденциальной является любая информация, с указанием стороны, которой принадлежит информация и имеющая гриф, свидетельствующий об отнесении сведений к информации конфиденциального характера, такой как: «Коммерческая тайна», «Конфиденциально», «Конфиденциальная информация» и т.п.

4. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ИНФОРМАЦИИ

4.1. Обработка сведений конфиденциального характера, подлежащих защите и ставших доступными Сторонам данного соглашения, должна осуществляться согласно следующим принципам:

- обработка сведений конфиденциального характера должна осуществляться на законной и справедливой основе и должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка сведений конфиденциального характера, несовместимая с целями сбора данных;
- не допускается объединение баз данных, содержащих сведения конфиденциального характера, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только сведения конфиденциального характера, которые отвечают целям их обработки;
- содержание и объем обрабатываемых сведений конфиденциального характера должны соответствовать заявленным целям обработки;
- хранение сведений конфиденциального характера должно осуществляться не дольше, чем этого требуют цели обработки данной информации. Сведения

конфиденциального характера подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

- сведения конфиденциального характера запрещается разглашать третьим лицам без письменного согласия Передающей стороны.

5. ПРАВА И ОБЯЗАННОСТИ СТОРОН

5.1. Каждая Сторона принимает на себя следующие обязательства:

- осуществлять обработку сведений конфиденциального характера, перечень которых указан в пункте 3 данного Соглашения, в соответствии с законодательством и иными нормативными документами Российской Федерации;
- осуществлять передачу сведений конфиденциального характера третьим лицам в соответствии с законодательством и иными нормативными документами Российской Федерации;
- соблюдать необходимый уровень защиты сведений конфиденциального характера в соответствии с законодательством и иными нормативными документами Российской Федерации;
- не использовать сведения конфиденциального характера другой Стороны, за исключением тех случаев, когда такое использование осуществляется в рамках совместных проектов и/или в целях исполнения обязательств по всем заключенным между Сторонами договорами;

5.2. Стороны договариваются о том, что будут исполнять свои обязанности по настоящему Соглашению без выплаты какого-либо вознаграждения друг другу.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Настоящее Соглашение вступает в силу с даты его подписания и действует по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

6.2. Обязательства по неразглашению Конфиденциальной информации и ее использованию, предусмотренные в настоящем Соглашении, остаются в силе в течение 60 (шестидесяти) месяцев для каждой единицы конфиденциальной информации с момента её раскрытия Принимающей стороне.

6.3. Настоящее Соглашение может быть изменено или дополнено только посредством письменного соглашения, заключенного Сторонами.

6.4. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из сторон.

7. АДРЕСА И РЕКВИЗИТЫ СТОРОН

Государственное бюджетное учреждение здравоохранения города Москвы Городская клиническая больница имени С.П. Боткина Департамента здравоохранения города Москвы	**Сторона-2**

Фактический адрес:	
Юридический адрес:	
Тел./факс:	
ИНН:	
КПП:	
ОГРН:	
БИК:	
Наименование банка	

Фактический адрес:	
Юридический адрес:	
Тел./факс:	
ИНН:	
КПП:	
ОГРН:	
БИК:	
Наименование банка	

ПОДПИСИ СТОРОН

Подписант

_____ */И.О. Фамилия/*

М.П

Подписант

_____ */И.О. Фамилия/*

М.П