

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ  
ГОРОДА МОСКВЫ

«ИНФЕКЦИОННАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА № 1  
ДЕПАРТАМЕНТА ЗДРАВООХРАНЕНИЯ ГОРОДА МОСКВЫ»

П Р И К А З

30.03.2018

№ 199

*Об Утверждении «Политики обработки персональных данных в Государственном бюджетном учреждении здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы» и иных локально-нормативных актов регламентирующих работу с персональными данными в ГБУЗ «ИКБ № 1 ДЗМ»*

В соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» и другими нормативными правовыми актами Российской Федерации

**ПРИКАЗЫВАЮ:**

1. Принять и утвердить «Политику обработки и защиты персональных данных в Государственном бюджетном учреждении здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы» (приложение 1 к настоящему приказу) (далее – Политика).
2. Политику ввести в действие с **02 апреля 2018 года**.
3. Принять и утвердить «Положение о защите персональных данных пациентов Государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы» (приложение 2 к настоящему приказу) (далее – Положение о защите персональных данных пациентов).
4. Положение о защите персональных данных пациентов ввести в действие с **02 апреля 2018 года**.
5. Принять и утвердить «Положение о работе с персональными данными работников Государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы» (приложение 3 к настоящему приказу) (далее – Положение о работе с персональными данными работников).
6. Положение о работе с персональными данными работников ввести в действие с **02 апреля 2018 года**.
7. Сотрудникам ГБУЗ «ИКБ №1 ДЗМ» в целях исполнения требований о неразглашении персональных данных, имеющим доступ к таким данным, руководствоваться Политикой, Положением о работе с персональными данными работников, а также Положением о защите персональных данных пациентов.

8. Всем сотрудникам не допускать лиц, не состоящих в трудовых отношениях с ГБУЗ «ИКБ № 1 ДЗМ», к совместным обследованиям и экспертизе до подписания ими «Обязательства о защите персональных данных и данных, составляющих врачебную тайну» (Приложение 1 к Положению о защите персональных данных пациентов государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы»).
9. Начальнику отдела кадров, совместно с заведующим канцелярии, обеспечить ознакомление сотрудников с данным Приказом, в срок по 03.05.2018 г. Листы ознакомления хранить в отделе кадров в отдельной папке.
10. Начальнику отдела кадров обеспечить подписание и хранение в личных делах «Обязательства о защите персональных данных и данных, составляющих врачебную тайну» в срок по 03.05.2018 г.
11. Контроль за выполнением п. 7 и п. 8 настоящего приказа возложить на руководителей структурных подразделений ГБУЗ «ИКБ № 1 ДЗМ».
12. Политику и Положение о защите персональных данных пациентов опубликовать на официальном сайте ГБУЗ «ИКБ № 1 ДЗМ» в срок до 16.04.2018 г.
13. Контроль за выполнением настоящего приказа оставляю за собой.

Главный врач



С.В. Сметанина



2.1. Персональными данными работника является любая информация, относящаяся к определенному или определяемому на основании такой информации работнику (субъекту персональных данных), а именно: фамилия, имя, отчество, год, месяц, дата и место рождения, анкетные и биографические данные, адрес, паспортные данные, номер домашнего телефона, семейное, социальное, имущественное положение, сведения о составе семьи, место работы или учебы членов семьи и родственников, наличие судимостей, образование, профессия, общий трудовой и медицинский стаж, социальные льготы, сведения, связанные с повышением квалификации и переподготовкой работников, их аттестацией, заработная плата работников, доходы, другая информация.

К персональным данным работника относятся сведения, содержащиеся в трудовом договоре, личных делах и трудовых книжках работников, в приказах по личному составу, воинском учете, в декларации о наличии материальных ценностей, в декларации, подаваемой в налоговую инспекцию, в документах, связанные со служебным расследованием, в отчетах, направляемые в органы статистики.

2.2. Персональные данные работника используются Организацией, в частности в целях выполнения требований:

- трудового законодательства и иных актов, содержащих нормы трудового права, при приеме на работу, при предоставлении гарантий и компенсаций и др.;
- налогового законодательства, в связи с исчислением и уплатой налога на доходы физических лиц, страховые выплаты в ФСС РФ и ПФР РФ;
- пенсионного законодательства при формировании и предоставлении персонализированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование.

2.3. К информации, содержащей персональные данные работника, применяется режим конфиденциальности, то есть обязательное для соблюдения, получившим доступ к персональным данным, лицом требование не допускать их распространения без согласия работника или наличия иного законодательного основания.

2.4. Не требуется обеспечение конфиденциальности персональных данных в случаях:

- обезличивания информации;
- общедоступности персональных данных.

2.5. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, предоставление (в том числе передача), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.6. Распространение персональных данных работника – это действия, направленные на передачу персональных данных определенному кругу лиц или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.7. Использование персональных данных работника – это действия (операции) с персональными данными, совершаемые получившим доступ к персональным данным лицом в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника или других лиц, либо иным образом затрагивающих права и свободы работника или других лиц.

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

2.9. Уничтожение персональных данных работника – это 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.

2.10. Обезличивание персональных данных работника – это действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику.

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

2.12. Общедоступные персональные данные работника- это персональные данные, доступ неограниченного круга лиц, к которым предоставлен с согласия работника или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.13. Доступ к персональным данным работника имеют должностные лица (далее-уполномоченные должностные лица) для выполнения своих функциональных обязанностей. Круг лиц, допущенных к работе с документами, содержащими персональные данные работников, определяется приказом главного врача Организации.

С работниками, ответственными за хранение персональных данных, а также с работниками, владеющими персональными данными в силу своих должностных обязанностей, заключаются Соглашения о неразглашении персональных данных работников, форма которого приложена в Приложении 1 настоящего Положения. Соглашение о неразглашении персональных данных работника хранится в личном деле работника.

2.14. При заключении трудового договора после ознакомления с настоящим Положением работник дает свое согласие на обработку персональных данных.

### 3. Доступ к персональным данным работника

3.1. Право доступа к персональным данным работника имеют:

- главный врач,
- заместители главного врача по направлениям деятельности имеют доступ к персональным данным работников только курируемых подразделений;
- начальник отдела кадров и работники отдела кадров;
- главный бухгалтер и работники бухгалтерии, отвечающие за расчет заработной платы работников больницы, кассовые операции, расчеты с подотчетными лицами;
- начальник планово-экономического отдела и его работники, связанные с трудовой деятельностью работников и их заработной платой;
- ведущий юрисконсульт;
- работники отдела, обеспечивающие работоспособность аппаратно-программных средств, предназначенных для автоматизированной обработки персональных данных, – к персональным данным, обрабатываемым данными аппаратно-программными средствами;
- руководители структурных подразделений имеют доступ к персональным данным только работников своего подразделения;
- доступ специалистов других отделов к персональным данным работников осуществляется на основании письменного разрешения главного врача, либо его заместителя;
- другие работники Организации имеют доступ к персональным данным работника, только с письменного согласия самого работника, носителя данных;
- работник, как носитель данных.

3.2. Внешний доступ. Массовые потребители персональных данных вне организации государственные и негосударственные функциональные структуры:

- налоговые инспекции (на законных основаниях);
- судебные и правоохранительные органы (в случаях, установленных законодательством);
- органы статистики (на законных основаниях);
- страховые агентства (на законных основаниях);
- военкоматы (на законных основаниях);
- органы социального страхования (на законных основаниях);
- пенсионные фонды (на законных основаниях);
- подразделения муниципальных органов управления (на законных основаниях);

- надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

### 3.3. Другие организации.

Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

Сведения о работающем работнике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника.

### 3.4. Родственники и члены семьи:

- персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника;

- в случае развода бывшая супруга (супруг) имеет право обратиться в Организацию с письменным запросом о размере заработной платы работника без его согласия (Трудовой кодекс Российской Федерации).

## 4. Получение и обработка персональных данных работников

4.1. Уполномоченные должностные лица получают все персональные данные работника непосредственно у самого работника. Если персональные данные работника можно получить только у третьего лица, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Уполномоченные должностные лица должны сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.2. При поступлении на работу работник предоставляет о себе следующие данные: фамилию, пол, дату и место рождения, семейное положение, образование, специальность, отношение к воинской обязанности, место жительства и телефоны для связи, а также иные сведения, необходимые для оформления личной карточки работника по унифицированной форме Т-2, и другие сведения, которые работник считает нужным сообщить. На личную карточку работника клеивается фотография работника.

4.3. Информация, содержащая персональные данные работника хранятся в личном деле работника. Формирование и ведение личных дел осуществляется работниками кадровой службы Организации.

4.4. Уполномоченные должностные лица не вправе требовать от работника представления информации о его политических и религиозных убеждениях, а также о частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, уполномоченные должностные лица вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

4.5. Уполномоченные должностные лица не вправе получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или о его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

4.6. Работник предоставляет уполномоченному должностному лицу достоверные сведения о себе. Уполномоченное должностное лицо проверяет достоверность сведений, сверяя данные, представленные работником, с имеющимися у работника документами.

4.7. При изменении персональных данных работник письменно уведомляет уполномоченное должностное лицо о таких изменениях не позднее 14 календарных дней с даты изменения персональных данных.

4.8. По мере необходимости Работодатель истребует у работника дополнительные сведения. Работник представляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

## **5. Носители персональных данных работников**

5.1. Личные дела и личные карточки работника Т-2 в бумажном виде хранятся в шкафах и ящиках столов, защищенных от несанкционированного доступа.

5.2. Трудовые книжки работников, вкладыши в них, журналы учета, бланки строгой отчетности хранятся в сейфах.

5.3. Другие документы на бумажных носителях, содержащие персональные данные работников хранятся в местах, защищенных от несанкционированного доступа.

5.4. Помещения в рабочее время при отсутствии в них работников, работающих с персональными данными, должны быть закрыты.

5.5. Проведение уборки помещения должно производиться в присутствии работников отдела кадров.

5.6. Персональные данные работников могут храниться в электронном виде в локальной компьютерной сети и персональных ЭВМ уполномоченных должностных лиц. Доступ к электронным носителям, содержащие персональные данные работников, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных.

5.5. Копировать и делать выписки из документов, содержащих персональные данные работника, разрешается уполномоченными должностными лицами исключительно в служебных целях.

## **6. Права работников**

6.1. Работнику предоставляется полная информация о его персональных данных и обработке этих данных.

6.2. На основании письменного заявления работника ему бесплатно выдаются копии документов, содержащих его персональные данные, за исключением случаев, предусмотренных федеральными законами.

6.3. Работник имеет право определять своих представителей для защиты собственных персональных данных.

6.4. Работник вправе требовать исключить или исправить неверные или неполные персональные данные, а также данные обработанные с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона. Персональные данные оценочного характера работник вправе дополнить заявлением, выражающим его собственную точку зрения.

6.5. Работник вправе требовать уполномоченных должностных лиц об извещении всех адресатов, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или добавлениях. Уполномоченные должностные лица Организации в срок 5-ти рабочих дней обязаны это сделать.

6.6. Работник имеет право обжаловать в соответствующие инстанции любые неправомерные действия или бездействие уполномоченных должностных лиц при обработке и защите его персональных данных.

6.7. Работник не должен отказываться от своих прав на сохранение и защиту тайны.

## **7. Использование персональных данных работников**

7.1. Персональные данные работника используются уполномоченными должностными лицами исключительно в целях обеспечения соблюдения нормативных правовых актов, содействия работников в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

7.2. При принятии решений, затрагивающих интересы работника, уполномоченные должностные лица не имеют права основываться на персональных данных работника,

полученных исключительно в результате их автоматизированной обработки или электронного получения. Уполномоченные должностные лица также не вправе принимать решения затрагивающие интересы работника, основываясь на данных, допускающих двойное толкование. В случае, если на основании персональных данных работника невозможно установить какой-либо факт, уполномоченное должностное лицо предлагает работнику представить письменные разъяснения.

7.3. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

## **8. Передача персональных данных работников**

8.1. Информация, относящаяся к персональным данным работников, может быть предоставлена органам в порядке, установленном федеральными законами.

8.2. Уполномоченные должностные лица не вправе предоставлять персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

8.3. Уполномоченные должностные лица предупреждают адресатов, получающих персональные данные работника о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдается. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами.

8.4. В случае, если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника, либо отсутствует письменное согласие работника на предоставление его персональных данных, уполномоченное должностное лицо обязано отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных. Копия уведомления подшивается в личное дело работника.

8.5. Персональные данные работника могут быть переданы представителю работника в порядке, установленном Трудовым кодексом Российской Федерации в том объеме, в каком это необходимо для выполнения указанным представителем их функций.

8.6. Уполномоченное должностное лицо обеспечивает ведение журнала учета передачи информации, содержащей персональные данные работников, в котором регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается какая именно информация была передана.

## **9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника**

9.1. Лица, виновные в нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

9.2. Если права и законные интересы работника были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с иском о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.



9.3. С лицами, виновными в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника может быть расторгнут трудовой договор на основании п.11 ст.81 Трудового кодекса Российской Федерации.

#### **10. Заключительные положения**

- 10.1. Настоящее Положение вступает в силу с даты его утверждения или с даты указанной в локальном нормативном акте Организации.
- 10.2. Положение обязательно для всех работников Организации, если иные условия не предусмотрены в трудовом договоре работника.
11. При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании Приказа главного врача ГБУЗ «ИКБ № 1 ДЗМ».

Приложение 1 к Положению о работе с персональными данными работников Государственного бюджетного учреждения здравоохранения города Москвы «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы»

## СОГЛАШЕНИЕ о неразглашении персональных данных работников

Я, \_\_\_\_\_, паспорт \_\_\_\_\_, выданный \_\_\_\_\_ " " \_\_\_\_\_ года.

понимаю, что получаю доступ к персональным данным работников ГБУЗ «ИКБ № 1 ДЗМ». Я также понимаю, что во время исполнения своих обязанностей мне приходится заниматься сбором, обработкой и хранением персональных данных работников.

Я понимаю, что разглашение такого рода информации может нанести ущерб работникам Организации, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными работника соблюдать все описанные в Положении о работе с персональными данными требования.

Я подтверждаю, что не имею права разглашать сведения о (об):

- анкетных и биографических данных;
- образовании;
- общем трудовом и медицинском стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате сотрудника;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- характере взаимоотношений в семье;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в налоговую инспекцию;
- подлинниках и копиях приказов по личному составу;
- содержащиеся в личных делах и трудовых книжках работников;
- о документах, содержащих сведения по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудника, или их утраты я несу ответственность в соответствии с ст. 90 ТК РФ.

С Положением о работе с персональными данными работников ГБУЗ «ИКБ № 1 ДЗМ», Политикой обработки и защиты персональных данных в Государственном бюджетном учреждении здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы» и гарантиях их защиты ознакомлен(а).

\_\_\_\_\_  
(должность)

" " \_\_\_\_\_ 20\_\_ г.

\_\_\_\_\_  
(Ф.И.О.)

\_\_\_\_\_  
подпись

Приложение 2 к Положению о работе с персональными данными работников Государственного бюджетного учреждения здравоохранения города Москвы «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы»

## СОГЛАСИЕ РАБОТНИКА на обработку персональных данных

Я, \_\_\_\_\_  
(Ф.И.О. полностью)

Зарегистрированный (ая) по адресу: \_\_\_\_\_

Документ, удостоверяющий личность \_\_\_\_\_ серия \_\_\_\_\_ № \_\_\_\_\_  
выдан \_\_\_\_\_

в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях: обеспечения соблюдения законов и иных нормативных правовых актов; заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений; отражения информации в кадровых документах; начисления заработной платы; исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование; представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ; а также статистической отчетности в Росстат предоставления сведений в кредитную организацию для оформления банковской карты и перечисления на нее заработной платы; предоставления сведений третьим лицам для оформления полиса ДМС; предоставления налоговых вычетов; обеспечения моей безопасности; контроля количества и качества выполняемой мной работы; обеспечения сохранности имущества работодателя даю согласие на обработку ГБУЗ «ИКБ № 1 ДЗМ» (далее – Оператор), расположенный по адресу: Москва, Волоколамское шоссе, д. 63 моих персональных данных, включающих: фамилия, имя, отчество; пол, возраст; дата и место рождения; паспортные данные; адрес регистрации по месту жительства и адрес фактического проживания; номер телефона (домашний, мобильный); данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации; семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством; отношение к воинской обязанности; сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы; сведения о ранее проведенных медицинских осмотрах (в случае, если они необходимы при приеме на работу); СНИЛС; ИНН; информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБУЗ «ИКБ № 1 ДЗМ»; сведения о доходах в ГБУЗ «ИКБ № 1 ДЗМ»; сведения о деловых и иных личных качествах, носящих оценочный характер.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, уничтожение персональных данных.

Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы,





Приложение 4 к Положению о работе с персональными данными работников Государственного бюджетного учреждения здравоохранения города Москвы «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы»

**СОГЛАСИЕ РАБОТНИКА  
на передачу персональных данных третьей стороне**

Я, \_\_\_\_\_  
(Ф.И.О. полностью)

Зарегистрированный (ая) по адресу: \_\_\_\_\_  
\_\_\_\_\_

Документ, удостоверяющий личность \_\_\_\_\_ серия \_\_\_\_\_

№ \_\_\_\_\_ выдан \_\_\_\_\_

в соответствии Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие ГБУЗ «ИКБ № 1 ДЗМ» (далее – Оператор), расположенный по адресу: Москва, Волоколамское шоссе, д. 63 на передачу моих персональных данных, включающих:

\_\_\_\_\_ (указать персональные данные)

в

\_\_\_\_\_ (указать организацию, учреждение, в которые передаются персональные данные)

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

/ \_\_\_\_\_ / \_\_\_\_\_  
(Подпись) (расшифровка)

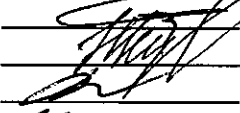
« \_\_\_\_\_ » \_\_\_\_\_ 201\_\_ г.

Приложение 2  
к приказу от «30» 05 2018 № 199

## СОГЛАСОВАНО

### От работников

Представительный орган из числа  
сотрудников ГБУЗ «ИКБ №1 ДЗМ»

  
Е.В. Власов  
Н.А. Курилова  
М.Г. Русанова

«30» марта 2018 г.

## УТВЕРЖДАЮ

### От работодателя



ГБУЗ  
«ИКБ №1 ДЗМ»

С.В. Сметанина

2018 г.

## ПОЛОЖЕНИЕ

### о защите персональных данных пациентов Государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы»

#### 1. Общие положения

1.1. Настоящее Положение о защите персональных данных пациентов государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы» (далее – Положение) определяет порядок создания, обработки и защиты персональных данных пациентов, их законных представителей и иных лиц, не являющихся работниками государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы» (далее Учреждение-оператор), чьи персональные данные хранятся и обрабатываются Учреждением-оператором, далее совместно именуемых «пациенты».

1.2. Основанием для разработки данного локального нормативного акта являются:

- ст. ст. 2. 17-24. 41 Конституции РФ от 12 декабря 1993 г.;
- ст. ст. 85-90 Трудового кодекса РФ;
- часть 1 и 2. часть 4 Гражданского кодекса РФ;
- Указ Президента РФ от 06 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;
- Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- Федеральный закон от 30 марта 1999 г. № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 17 сентября 1998 г. № 157-ФЗ (ред. от 24 июля 2010 г.) «Об иммунопрофилактике инфекционных болезней»;
- Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 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»;
- Постановление Правительства Российской Федерации от 06 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем»

- персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
  - 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»;
  - Приказ Минздрава РФ от 15 октября 1999 № 377 (ред. от 12.04.2007) «Об утверждении положения об оплате труда работников здравоохранения» (Зарегистрировано в Минюсте РФ 21.10.1999 № 1943);
  - Регламентирующие документы ФСТЭК России и ФСБ России об обеспечении безопасности персональных данных:
  - «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15 февраля 2008 г.);
  - Лицензия на осуществление медицинской деятельности № ЛО-77-01-014369 от 05.06.2017 (бессрочная) выдана Департаментом здравоохранения города Москвы;
- 1.1. Целью настоящего Положения является определение порядка хранения и обработки персональных данных пациентов, обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным пациентов, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.
- 1.2. Персональные данные пациентов относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере негосударственной (служебной, профессиональной) тайны.

## **2. Основные понятия, используемые в настоящем Положении**

Для целей настоящего Положения применяются следующие термины и определения:

*Оператор* - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

*Пациенты* (субъекты персональных данных) - физические лица и их законные представители, обратившиеся в Учреждение-оператор с целью получения медицинского обслуживания, либо состоящие в иных гражданско-правовых отношениях с Учреждением-оператором, не являющиеся работниками Учреждения-оператора.

*Врачебная тайна* - соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении.

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

*Документы, содержащие персональные данные пациента* - документы, необходимые для осуществления действий в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, а также для оформления договорных отношений.

*Обработка персональных данных пациента* - 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 пациента.

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

*Предоставление персональных данных* - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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

*Уничтожение персональных данных* - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

*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.

*Конфиденциальность персональных данных* - операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

*Несанкционированный доступ (несанкционированные действия)* - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами 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 Федеральным законодательством не распространяется требование соблюдения конфиденциальности.

### **3. Общие принципы и условия обработки персональных данных пациентов**

3.1 Обработка персональных данных пациента осуществляется на основе следующих принципов:

- а) Обработка персональных данных должна осуществляться на законной и справедливой основе.
- б) Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- в) Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- г) Обработке подлежат только персональные данные, которые отвечают целям их обработки
- д) 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.
- е) При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждение-оператор должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

ж) 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 № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законодательством.

3.2 В целях обеспечения прав и свобод человека и гражданина Учреждение-оператор и его представители при обработке персональных данных пациента обязаны соблюдать следующие общие требования:

1) Обработка персональных данных пациентов может осуществляться исключительно в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, оформления договорных отношений с пациентом при условии, что обработка персональных данных осуществляется лицом, обязанным сохранять врачебную тайну в соответствии с законодательством Российской Федерации.

2) Все персональные данные пациента следует получать у него самого или у его полномочного представителя. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

3) При определении объема и содержания обрабатываемых персональных данных пациента, Учреждение-оператор должно руководствоваться Конституцией Российской Федерации, Федеральным законом № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», законодательством РФ в сфере защиты персональных данных и обработки информации, Уставом Учреждения-оператора и иными локальными нормативными актами в области защиты персональных данных.

4) Учреждение-оператор не имеет права получать и обрабатывать персональные данные пациента, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

5) Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении пациента или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

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

7) Учреждение-оператор обязано разъяснить пациенту и его законному представителю порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты пациентом своих прав и законных интересов.

8) Учреждение-оператор обязано рассмотреть возражение в течение тридцати дней со дня его получения и уведомить пациента о результатах рассмотрения такого возражения.

9) Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Учреждением-оператором за счет своих средств, в порядке, установленном Федеральным законодательством и другими нормативными документами.

3.3 Учреждение-оператор вправе поручить обработку персональных данных другому лицу с

согласия пациента, если иное не предусмотрено Федеральным законом № 152-ФЗ, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение Учреждения-оператора). Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении Учреждения-оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ.

3.4 Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, не обязано получать согласие пациента на обработку его персональных данных.

3.5 В случае если Учреждение-оператор поручает обработку персональных данных другому лицу, ответственность перед пациентом за действия указанного лица несет Учреждение-оператор. Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, несет ответственность перед Учреждением-оператором.

#### **4. Получение персональных данных пациента**

4.1 Получение персональных данных преимущественно осуществляется путем представления законным представителем пациента либо самим пациентом на основании его письменного согласия, за исключением случаев, прямо предусмотренных действующим законодательством РФ.

В случаях, предусмотренных Федеральным законодательством, обработка персональных данных осуществляется только с согласия законного представителя пациента или пациента в письменной форме. Равнозначным содержащему собственноручную подпись пациента согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом № 152-ФЗ электронной подписью. Согласие пациента в письменной форме на обработку его персональных данных должно включать в себя, в частности:

- 1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- 2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- 3) наименование и адрес Учреждения-оператора (ГБУЗ «ИКБ №1 ДЗМ»), а также фамилию, имя, отчество и должность работника Учреждения-оператора, получающего согласие субъекта персональных данных;
- 4) цель обработки персональных данных;
- 5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- 6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения-оператора, если обработка будет поручена такому лицу;
- 7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением-оператором способов обработки персональных данных;
- 8) срок, в течение которого действует согласие субъекта персональных данных, а также

способ его отзыва, если иное не установлено Федеральным законодательством;

9) подпись субъекта персональных данных.

Для обработки персональных данных, содержащихся в согласии пациента в письменной форме на обработку его персональных данных, дополнительное согласие не требуется.

В случае недееспособности пациента или не достижения пациентом возраста 15 лет согласие на обработку его персональных данных дает в письменной форме его законный представитель.

4.2 В случае необходимости проверки персональных данных пациента Учреждение-оператор заблаговременно должен сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

## **5. Хранение и использование персональных данных пациентов**

5.1 Информация персонального характера пациента хранится и обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

5.2. Обработка персональных данных пациентов Учреждения-оператора осуществляется смешанным путем:

- неавтоматизированным способом обработки персональных данных;
- автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

5.3 Персональные данные пациентов хранятся на бумажных носителях и в электронном виде.

5.4 Документы, содержащие персональные данные пациентов Учреждения-оператора, хранятся в отделе госпитализации, регистратуре консультативно-поликлинического отдела, отделениях стационара, в бухгалтерии.

5.5. Ответственные лица за хранение оконченных производством документов, содержащих персональные данные пациентов, назначаются Приказом главного врача ГБУЗ «ИКБ № 1 ДЗМ».

5.6 Возможна передача персональных данных пациентов по внутренней сети организации с использованием технических и программных средств защиты информации, с доступом только для работников Учреждения-оператора, допущенных к работе с персональными данными пациентов Приказом главного врача ГБУЗ «ИКБ № 1 ДЗМ» и только в объеме, необходимом данным работникам для выполнения своих должностных обязанностей. В должностные инструкции данных работников включается пункт об обязанности сохранения информации, являющейся конфиденциальной.

5.7 Хранение персональных данных пациентов осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение документов, содержащих персональные данные пациентов, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению.

5.8 Учреждение-оператор обеспечивает ограничение доступа к персональным данным пациентов лицам, не уполномоченным Федеральным законодательством, либо работодателем для получения соответствующих сведений.

## **6. Защита персональных данных пациентов**

6.1 Учреждение-оператор при обработке персональных данных пациентов обязано 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.

6.2 Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

6.3 Обеспечение безопасности персональных данных пациентов достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) 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;
- 3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 4) учетом машинных носителей персональных данных;
- 5) 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.

6.4 Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона № 152-ФЗ «О персональных данных».

6.5 Выбор средств защиты информации для системы защиты персональных данных осуществляется в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона № 152-ФЗ «О персональных данных».

6.6. Для обеспечения безопасности персональных данных пациентов при неавтоматизированной обработке предпринимаются следующие меры:

6.6.1. Определяются места хранения персональных данных (согласно настоящего Положения), которые оснащаются следующими средствами защиты:

- в кабинетах, где осуществляется хранение документов, содержащих персональные данные пациентов, имеются шкафы, стеллажи, сейфы;
- дополнительно кабинеты, где осуществляется хранение документов, содержащих персональные данные пациентов, оборудованы замками и системами пожарной сигнализации.
- Учреждение-оператор использует услуги вневедомственной охраны.

6.6.2. Все действия при неавтоматизированной обработке персональных данных пациентов осуществляются только должностными лицами Учреждения-оператора, согласно Списка должностей, штатного расписания и должностных инструкций, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

Данный Список должностей работников предусматривает замещение указанных должностей работников в соответствии с пп. «б» п. 1 Постановления Правительства Российской Федерации от 21.03. 2012 г. №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».

6.6.3. При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых, заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

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

2) 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.

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

Персональные данные пациентов, содержащиеся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных.

Эти правила применяются также в случае, если необходимо обеспечить отдельную 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, а если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

6.6.4 Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.7. Для обеспечения безопасности персональных данных пациентов при автоматизированной обработке предпринимаются следующие меры:

6.7.1 Все действия при автоматизированной обработке персональных данных пациентов осуществляются только должностными лицами Учреждения-оператора в соответствии со штатным расписанием и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

6.7.2. Персональные компьютеры, имеющие доступ к базам хранения персональных данных пациентов, защищены паролями доступа. Пароли устанавливаются сотрудником технического отдела Учреждения-оператора и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных пациентов на данном ПК.

6.7.3. Иные меры, предусмотренные Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

6.8. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с Приказами по архивному делу, или продлевается на основании заключения экспертной комиссии Учреждения-оператора, если иное не определено законодательством РФ.

## **7. Передача персональных данных пациентов третьим лицам**

7.1 Передача персональных данных пациентов третьим лицам осуществляется Учреждением-оператором только с письменного согласия пациента, за исключением случаев,

если:

- 1) передача необходима для защиты жизни и здоровья пациента, либо других лиц, и получение его согласия невозможно;
- 2) в целях обследования и лечения пациента, не способного из-за своего состояния выразить свою волю;
- 3) по запросу органов дознания, следствия, прокуратуры и суда в связи с проведением расследования или судебным разбирательством, в соответствии с Законом об оперативно-розыскной деятельности;
- 4) в случае оказания помощи несовершеннолетнему в возрасте до 15 лет, для информирования его родителей или законных представителей;
- 5) при наличии оснований, позволяющих полагать, что права и интересы пациента могут быть нарушены противоправными действиями других лиц;
- 6) в иных случаях, прямо предусмотренных Федеральным законодательством.

Лица, которым в установленном Федеральным законом № 152-ФЗ порядке переданы сведения, составляющие персональные данные пациента, несут дисциплинарную, административную или уголовную ответственность за разглашение в соответствии с законодательством Российской Федерации.

7.2 Передача персональных данных пациента третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой главного врача ГБУЗ «ИКБ № 1 ДЗМ» при условии соблюдения требований, предусмотренных п. 7.1 настоящего Положения.

Учреждение-оператор обеспечивает ведение Журнала учета выданных персональных данных пациентов по запросам, в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

В случае если лицо, обратившееся с запросом, не уполномочено Федеральным законодательством на получение персональных данных пациента, либо отсутствует письменное согласие пациента на передачу его персональных данных, Учреждение-оператор обязано отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдается мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится у Учреждения- оператора.

## **8. Общедоступные источники персональных данных пациентов**

8.1 Включение персональных данных пациента в общедоступные источники персональных данных возможно только при наличии его письменного согласия.

8.2 При обезличивании персональных данных согласие пациента на включение персональных данных в общедоступные источники персональных данных не требуется.

8.3 Введения о пациентах могут быть исключены из общедоступных источников персональных данных по требованию самого пациента, либо по решению суда или иных уполномоченных государственных органов.

## **9. Права и обязанности пациента в области защиты его персональных данных**

9.1 В целях обеспечения защиты персональных данных, хранящихся у Учреждения-оператора, пациенты имеют право на:

- полную информацию о составе и содержимом их персональных данных, а также способе обработки этих данных;
- свободный доступ к своим персональным данным.

Пациент имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Учреждением-оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые Учреждением-оператором способы обработки персональных данных;
- 4) наименование и место нахождения Учреждения-оператора, сведения о лицах (за

исключением работников Учреждения-оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением-оператором или на основании Федерального закона № 152-ФЗ;

- 5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;
- 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения-оператора, если обработка поручена или будет поручена такому лицу;
- 10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или Федеральным законодательством.

Сведения должны быть предоставлены пациенту или законному представителю пациента Учреждением-оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

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

В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления пациенту по его запросу, пациент вправе обратиться повторно к Учреждению-оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

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

9.2 В случае выявления неправомерной обработки персональных данных при обращении пациента или его законного представителя, либо по запросу пациента или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных. Учреждение-оператор обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) с



момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении пациента или его законного представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение-оператор обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы пациента или третьих лиц.

9.3 В случае подтверждения факта неточности персональных данных Учреждение-оператор на основании сведений, представленных пациентом или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

9.4 В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением-оператором (или лицом, действующим по поручению Учреждения-оператора), Учреждение-оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения-оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение-оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение-оператор обязано уведомить пациента или его законного представителя, а в случае, если обращение пациента или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

9.5 В случае достижения цели обработки персональных данных Учреждение-оператор обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) 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 пациент, иным соглашением между Учреждением-оператором и пациентом, либо если Учреждение-оператор не вправе осуществлять обработку персональных данных без согласия пациента на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

9.6 В случае отзыва пациентом согласия на обработку его персональных данных Учреждение-оператор обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением-оператором и пациентом, либо если

Учреждение-оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

9.7 В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Учреждение-оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законодательством.

9.8 Для своевременной и полной реализации своих прав, пациент обязан предоставить Учреждению-оператору достоверные персональные данные.

## **10. Право на обжалование действий или бездействия Учреждения-оператора**

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

Пациент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке. Моральный вред, причиненный пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации.

Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

## **11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных пациентов**

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральным законодательством.

11.2. Работники ГБУЗ «ИКБ № 1 ДЗМ», допущенные к обработке персональных данных пациентов, за разглашение полученной в ходе своей трудовой деятельности информации, несут ответственность в соответствии с действующим законодательством Российской Федерации.

## **12. Заключительные положения**

12.1. Настоящее Положение вступает в силу с даты его утверждения или с даты указанной в локальном нормативном акте ГБУЗ «ИКБ № 1 ДЗМ».

12.2. При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании Приказа главного врача ГБУЗ «ИКБ № 1 ДЗМ».

12.3. Настоящее Положение распространяется на всех работников ГБУЗ «ИКБ № 1 ДЗМ», имеющих доступ и осуществляющих перечень действий с персональными данными пациентов. Пациенты ГБУЗ «ИКБ № 1 ДЗМ», а также их законные представители имеют право ознакомиться с настоящим Положением.

12.4. В обязанности работников, осуществляющих первичный сбор персональных данных пациента, входит получение согласия пациента на обработку его персональных данных под личную подпись

Приложение 1 к Положению о защите персональных данных пациентов государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы»

**Обязательство**  
**о неразглашении персональных данных пациентов и данных, составляющих врачебную тайну, полученных в ГБУЗ «ИКБ № 1 ДЗМ»**

Я,

---

*(Фамилия Имя Отчество)*

как сотрудник ГБУЗ «ИКБ № 1 ДЗМ», ИНН \_\_\_\_\_, ОГРН \_\_\_\_\_, в период трудовых отношений и после их окончания обязуюсь не разглашать персональные данные пациентов, обрабатываемые в ГБУЗ «ИКБ № 1 ДЗМ», которые будут мне доверены или станут мне известны в ходе исполнения должностных обязанностей и данных, составляющих врачебную тайну полученных в ГБУЗ «ИКБ № 1 ДЗМ».

Мне известно, что нарушение требований законодательства Российской Федерации в области персональных данных может повлечь дисциплинарную, административную, гражданско-правовую или уголовную ответственность согласно п.1 ст. 24 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных» и ст. 90 гл. 14 Трудового Кодекса Российской Федерации.

Я также подтверждаю, что ознакомлен с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику ГБУЗ «ИКБ № 1 ДЗМ» в отношении обработки персональных данных, локальными актами по вопросам обработки и обеспечения безопасности персональных данных.

« \_\_\_ »

20 г.

---

(должность)

---

(подпись)

---

(ФИО)

Приложение 2 к Положению о защите персональных данных пациентов государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы»

## СОГЛАСИЕ на обработку персональных данных

Я, нижеподписавшийся (аяся) «Пациент» \_\_\_\_\_

(Ф.И.О.),

в соответствии с требованиями ст. 9 Федерального закона от 27.07.06 г. «О персональных данных» №152-ФЗ, подтверждаю свое согласие на обработку в ГБУЗ «ИКБ № 1 ДЗМ» (далее – Оператор) персональных данных «Пациента», включающих: фамилию, имя, отчество, пол, дату рождения, адрес проживания, контактный телефон, реквизиты полиса ОМС (ДМС), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), данные о состоянии здоровья «Пациента», заболеваниях, случаях обращения за медицинской помощью, – в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания Оператором мне медицинской помощи я предоставляю право медицинским работникам, передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора, в интересах моего обследования и лечения.

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

Оператор имеет право во исполнение своих обязательств по работе в системе ОМС (по договору ДМС) на обмен (прием и передачу) моими персональными данными со страховой медицинской организацией ДМС и территориальным фондом ОМС с использованием машинных носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будут осуществляется лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет для стационара, пять лет – для поликлиники.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия или в случаях предусмотренных действующим законодательством Российской Федерации.

Настоящее согласие дано мной в дату подписания договора и действует бессрочно.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

«Пациент»

Фамилия, имя, отчество: \_\_\_\_\_

Адрес места жительства: \_\_\_\_\_

Телефон: \_\_\_\_\_

E-mail: \_\_\_\_\_

Паспорт: серия \_\_\_\_\_ № \_\_\_\_\_, выдан \_\_\_\_\_

« \_\_\_\_ » \_\_\_\_\_ г. код подразделения \_\_\_\_\_

Подпись: \_\_\_\_\_

Медицинский работник:

\_\_\_\_\_ (

должность)

Подпись: \_\_\_\_\_ / \_\_\_\_\_

(расшифровка подписи (Ф.И.О.)

СОГЛАСОВАНО

УТВЕРЖДАЮ

От работников

От работодателя


Представительный орган из числа  
сотрудников ГБУЗ «ИКБ №1 ДЗМ»

Главный врач ГБУЗ

 Е.В. Власов

«ИКБ №1 ДЗМ»

С.В. Сметанина

 Н.А. Курилова

2018 г.

 М.Г. Русанова

« 30 » марта 2018 г.

**Политика  
обработки и защиты персональных данных  
в Государственном бюджетном учреждении здравоохранения  
«Инфекционная клиническая больница № 1 Департамента здравоохранения  
города Москвы»**

**1. Общие положения**

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) составлена в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с пунктом 2 статьи 18.1 Закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных», другими нормативными правовыми актами Российской Федерации и является основополагающим внутренним регулятивным документом Государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы» (далее ГБУЗ «ИКБ № 1 ДЗМ» или Учреждение или Оператор), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее – ПД), оператором которым является Учреждение.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПД и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПД в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПД, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПД, полученных до ее утверждения.

1.4. Обработка ПД в Учреждении осуществляется в связи с выполнением Организацией функций, предусмотренных ее учредительными документами и определяемых:

- Законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановлением Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПД в Учреждении осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Учреждение выступает в качестве работодателя (гл. 14 ТК РФ), в связи с реализацией Организацией своих прав и обязанностей как юридического лица.

1.5. Учреждение имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата последнего обновления редакции. Новая редакция Политики вступает в силу с момента ее размещения на сайте, если иное не предусмотрено новой редакцией Политики.

1.6. Действующая редакция хранится в месте нахождения Учреждения по адресу: Москва, Волоколамское шоссе, д. 63, **Отдел кадров**, электронная версия Политики – на сайте по адресу: [ikb1.ru](http://ikb1.ru).

## 2. Термины и принятые сокращения

**Персональные данные (ПД)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (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.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

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

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

**Пациент** – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния.

**Медицинская деятельность** – профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях.

**Лечащий врач** – врач, на которого возложены функции по Учреждению и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения.

### **3. Принципы обеспечения безопасности персональных данных**

3.1. Основной задачей обеспечения безопасности ПД при их обработке в Учреждении является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПД, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПД Учреждение руководствуется следующими принципами:

- законность: защита ПД основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПД;
- системность: обработка ПД в Учреждении осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПД;
- комплексность: защита ПД строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Учреждения и других имеющихся в Учреждении систем и средств защиты;
- непрерывность: защита ПД обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПД, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПД, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПД осуществляется на основании результатов анализа практики обработки ПД в Учреждении с учетом выявления новых способов и средств реализации угроз безопасности ПД, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПД возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПД;
- минимизация прав доступа: доступ к ПД предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПД при изменении характеристик функционирования информационных систем персональных данных Учреждения, а также объема и состава обрабатываемых ПД;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПД осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;
- эффективность процедур отбора кадров: кадровая политика Учреждения предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПД;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПД должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПД, а результаты контроля регулярно анализируются.

3.3. В Учреждении не производится обработка ПД, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПД в Учреждении, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Организацией ПН уничтожаются или обезличиваются.

3.4. При обработке ПД обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уточнению неполных или неточных ПД.

## **4. Обработка персональных данных**

### **4.1. Получение ПД**

4.1.1. Все ПД следует получать от самого субъекта. Если ПД субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

4.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПД, характере подлежащих получению ПД, перечне действий с ПД, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получение.

4.1.3. Документы, содержащие ПД, создаются путем:

а) копирования оригиналов документов (паспорт, документ об образовании, свидетельство ИНН, пенсионное свидетельство и т. д.);

б) внесения сведений в учетные формы;

в) получения оригиналов необходимых документов (трудовая книжка, медицинское заключение, характеристика и т. д.).

Порядок доступа субъекта ПД к его ПД, обрабатываемым Организацией, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Учреждения.

### **4.2. Обработка ПД**

#### **4.2.1. Обработка персональных данных осуществляется:**

– с согласия субъекта персональных данных на обработку его персональных данных;

– в случаях, когда обработка персональных данных необходима для осуществления и выполнения возложенных законодательством Российской Федерации функций, полномочий и обязанностей;

– в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее – персональные данные, сделанные общедоступными субъектом персональных данных).

Доступ Работников к обрабатываемым ПД осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Учреждения.

Допущенные к обработке ПД Работники под подпись знакомятся с документами Учреждения, устанавливающими порядок обработки ПД, включая документы, устанавливающие права и обязанности конкретных Работников.

Организацией производится устранение выявленных нарушений законодательства об обработке и защите ПД.

#### **4.2.2. Цели обработки ПД:**

– обеспечение Учреждением оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими Учреждениями платных медицинских услуг, утвержденными постановлением Правительства РФ от 4 октября 2012 г. № 1006;



- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

#### **4.2.3. Категории субъектов персональных данных**

В Учреждении обрабатываются ПД следующих субъектов:

- физические лица, состоящие с учреждением в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за медицинской помощью.

#### **4.2.4. ПД, обрабатываемые Организацией:**

- полученные при осуществлении трудовых отношений;
- полученные для осуществления отбора кандидатов на работу в организацию;
- полученные при осуществлении гражданско-правовых отношений;
- полученные при оказании медицинской помощи.

**Полный список ПД представлен в:**

- Положении о работе с персональными данными работников Государственного бюджетного учреждения здравоохранения города Москвы «Инфекционная клиническая больница №1 Департамента здравоохранения города Москвы»;
- Положении о защите персональных данных пациентов государственного бюджетного учреждения здравоохранения «Инфекционная клиническая больница № 1 Департамента здравоохранения города Москвы».

#### **4.2.5. Обработка персональных данных ведется:**

- с использованием средств автоматизации;
- без использования средств автоматизации.

### **4.3. Хранение ПД**

4.3.1. ПД субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

4.3.2. ПД, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа (регистратура).

4.3.3. ПД субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

4.3.4. Не допускается хранение и размещение документов, содержащих ПД, в открытых электронных каталогах (файлообменниках) в ИСПД.

4.3.5. Хранение ПД в форме, позволяющей определить субъекта ПД, осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

### **4.4. Уничтожение ПД**

4.4.1. Уничтожение документов (носителей), содержащих ПД, производится путем сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение shreddera.

4.4.2. ПД на электронных носителях уничтожаются путем стирания или форматирования носителя.

4.4.3. Уничтожение производится комиссией. Факт уничтожения ПД подтверждается документально актом об уничтожении носителей, подписанным членами комиссии.

### **4.5. Передача ПД**

#### **4.5.1. Учреждение передает ПД третьим лицам в следующих случаях:**

- субъект выразил свое согласие на такие действия;
- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

#### **4.5.2. Перечень третьих лиц, которым передаются ПД:**

- Пенсионный фонд РФ для учета (на законных основаниях);

- Налоговые органы РФ (на законных основаниях);
- Фонд социального страхования (на законных основаниях);
- Территориальный фонд обязательного медицинского страхования (на законных основаниях);
- страховые медицинские Учреждения по обязательному и добровольному медицинскому страхованию (на законных основаниях);
- банки для начисления заработной платы (на основании договора);
- судебные и правоохранительные органы в случаях, установленных законодательством;
- бюро кредитных историй (с согласия субъекта);
- юридические компании, работающие в рамках законодательства РФ, при неисполнении обязательств по договору займа (с согласия субъекта).

## **5. Защита персональных данных**

5.1. В соответствии с требованиями нормативных документов Учреждением создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, публикаторской и рекламной деятельности, аналитической работы.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПД.

5.5. Основными мерами защиты ПД, используемыми Учреждением, являются:

5.5.1. Назначение лица ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением учреждением и его работниками требований к защите ПД.

5.5.2. Определение актуальных угроз безопасности ПД при их обработке в ИСПД и разработка мер и мероприятий по защите ПД.

5.5.3. Разработка политики в отношении обработки персональных данных.

5.5.4. Установление правил доступа к ПД, обрабатываемым в ИСПД, а также обеспечения регистрации и учета всех действий, совершаемых с ПД в ИСПД.

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

5.5.6. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, учет машинных носителей ПД, обеспечение их сохранности.

5.5.7. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

5.5.8. Сертифицированное программное средство защиты информации от несанкционированного доступа.

5.5.9. Сертифицированные межсетевой экран и средство обнаружения вторжения.

5.5.10. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ, оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПД.

5.5.11. Установление правил доступа к обрабатываемым ПД, обеспечение регистрации и учета действий, совершаемых с ПД, а также обнаружение фактов несанкционированного доступа к персональным данным и принятия мер.

5.5.12. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.5.13. Обучение работников Учреждения, непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о

персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Учреждения в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных.

5.5.14. Осуществление внутреннего контроля и аудита.

## **6. Основные права субъекта ПД и обязанности Учреждения**

### **6.1. Основные права субъекта ПД**

Субъект ПД имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые оператором способы обработки персональных данных;
- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные настоящим Законом или другими федеральными законами.

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

### **6.2. Обязанности Учреждения**

Учреждение обязана:

- при сборе ПД предоставить информацию об обработке его ПД;
- в случаях, если ПД были получены не от субъекта ПД, уведомить субъекта;
- при отказе в предоставлении ПД субъекту разъясняются последствия такого отказа;
- опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД, к сведениям о реализуемых требованиях к защите ПД;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД;
- давать ответы на запросы и обращения субъектов ПД, их представителей и уполномоченного органа по защите прав субъектов ПД.